# Staff Report of Public Comment Proceeding

| Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report | |
|---|---|
| **Publication Date:** | 22 April 2020 |
| **Prepared By:** | Jennifer Bryce |

| Public Comment Proceeding | |
|---|---|
| Open Date: | 24 January 2020 |
| Close Date: | 4 March 2020<br>Extended to 20 March 2020 |
| Staff Report Due Date: | 3 April 2020<br>Extended to 17 April 2020 |

| 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 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.

Formally convened in February 2017, the second Security, Stability, and Resiliency Review Team (SSR2) is assessing, as mandated by the Bylaws: *"ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates."*

As required by the ICANN Bylaws, the SSR2 Review Team posted its draft report for Public Comment on 24 January 2020.

***Next Steps:*** The SSR2 Review Team will carefully consider comments received and amend the report as it deems appropriate and in the public interest before submitting its final report to the Board. The final report will be published for Public Comment in advance of the Board's consideration.

## Section II: Contributors

*At the time this report was prepared, a total of eighteen (18) 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.*

Organizations and Groups:

| Name | Submitted by | Initials |
|---|---|---|
| Business Constituency | Steve DelBianco | BC |
| Root Serve System Advisory Committee | Andrew McConachie | RSSAC |
| I2Coaltion | Christian Dawson | I2 |
| Messaging, Malware, and Mobile Anti Abuse Working Group | Nat Kopcyk | M3AAG |
| Security and Stability Advisory Committee | Danielle Rutherford | SSAC |
| FIRST | Serge Droz | FIRST |
| Non-Commercial Stakeholder Group | Rafik Dammak | NCSG |
| At-Large Advisory Committee | ICANN At-Large staff | ALAC |
| MarkMonitor | Prudence Malinki | MM |
| ICANN Board | Wendy Profit | BD |
| Registrars Stakeholder Group | Zoe Bonython | RrSG |
| World Intellectual Property Organization | Brian Beckham | WIPO |
| ICANN Organization | Jennifer Bryce | ORG |
| Government Advisory Committee | Fabien Betremieux | GAC |
| Registries Stakeholder Group | Samantha Demetriou | RySG |
| Intellectual Property Constituency | Brian Scarpelli | IPC |

Individuals:

| Name | Affiliation (if provided) | Initials |
|---|---|---|
| Wolfgang Kleinwachter | Wolfgang Kleinwachter | WK |
| Loganaden Velvindron | Loganaden Velvindron | LV |

## 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).*

**BC:** The BC concurs with R.1 – R.31 and notes additional details around some of the recommendations. The BC also makes the following overarching comments:

"The BC supports the recommendations detailed in the report and, further to our longstanding advocacy for mitigating DNS abuse, is pleased to see that many of the RT's recommendations address this problem."

"SSR1 recommendations must be fully implemented if SSR2 recommendations are to have full impact."

"The SSR2 RT has done a commendable job in tailoring recommendations to address abuse-related issues."

"Independent oversight of ICANN efforts cannot be abridged. The BC echoes here its input on the Third Accountability and Transparency Review Team (ATRT3) draft report, where it called specifically for the continuation of meaningful and frequent community review of ICANN actions."

**RSSAC:** RSSAC "limits its comments to its remit (i.e., the recommendations on Key Signing Key rollover, root server operations)." Operating with this approach, the RSSAC expressed support for R.20, 21 and 22.

**I2:** I2 believes "the recommendations go beyond what is appropriate for a Review Team in terms of scope. Overreaches include dictating changes to the RAA and RA and other policy-based recommendations, and/or recommendations that in effect work against efforts of PDPs already underway."

I2 notes "the recommendations overreach [the review team's] remit, in terms of ICANN's governance and functioning mechanisms, as they advocate in a number of recommendations for unilateral, top-down action from the Board or ICANN Org on new and/or under-development policy matters. Specifically, recommendation 10 (Improve the Framework to Define and Measure Registrar & Registry Compliance) which is rated with a High Importance, and has among its sub-recommendations unilaterally amending contract clauses (10.3) and closing the EPDP while unilaterally implementing a new WHOIS policy (10.4). Further, recommendation 12 outright describes the direct and sole role that the Board should play in the creation of legal and appropriate access mechanisms to WHOIS data. Even more, recommendations 15 and 16 argue for "enhancing" and "changing" contracts, respectively. All three recommendations, 12, 15 and 16 are rated High Importance."

**M3AAG:** M3AAG "concur[s] with the SSR2 RT assertion that 'the publications, statements, and related actions by the ICANN organization have consistently understated or omitted the impact of systemic abuse of the DNS and its use as a platform for launching systematic attacks on individual and organizational systems worldwide'". M3AAG continues, "the report should further urge the ICANN organization to be transparent and to exercise its ability to negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission."

M3AAG makes the following additional comments:

"The ICANN organization and community should commit publicly to complete [SSR1 RT recommendations and other, prior recommendations] implementations as a matter of urgency and global necessity."

"We concur with the SSR2 RT regarding ICANN's failure to request, enumerate, or to negotiate for enforcement tools."

"We recommend that the SSR2 RT urge ICANN to adopt a contract negotiation process in which the influence of contracted parties who pay fees to ICANN cannot be held in question."

"We urge the SSR2 RT to recommend that contracted parties be obligated *by contract* to accommodate the high-volume needs of operational security users. Mechanisms such as whitelisting, vetting or pre-authorization which unfairly encumber academics, individuals who responsibly investigate abuse, and generally any party who has legitimate purposes to collect registration data, should not be used."

"M3AAG concurs with the SSR2 RT regarding publication of registry and registrar abuse statistics from DAAR. We recommend that the SSR2 make clear that rate limiting is an impediment to the DAAR system's ability to accurately report registrar statistics."

"We urge the team to consistently "Ensure access to registration data for parties with legitimate purposes" which most accurately identifies the parties with need to access registration data. We further urge the review team to recommend that ICANN take no action to sunset Whois until it has determined that RDAP services are reliable, available and accurate. Lastly, we recommend that the Review Team request ICANN to conduct a study of the various (inter)relationships between registrar implementations to satisfy the EU GDPR and California's CCPA and the privacy or proxy protection services, and to publish or establish uniform criteria for processes to obtain underlying registration data when redacted or hidden by a privacy/proxy protection service (or in some cases, both)."

"We concur with the SSR2 RT recommendation that ICANN should study pricing, yet urge the review team to further ask that registries and registrars share pricing with ICANN as a matter of contract, and that ICANN publish pricing at its web site, in machine usable formats."

"We urge the SSR2 team to call for further economic modeling and study of the DNS economy by qualified professionals instead of explicit pricing recommendations."

**SSAC:** SSAC makes the following general comments:

"Some SSAC reviewers believe that it would be helpful for the community and helpful in terms of overall accountability for SSR2 to have included an assessment of the extent to which the ICANN community, ICANN Board, and ICANN org are operating effectively from a security and stability perspective."

"It would be helpful if the SSR2 RT provided context and reasoning to substantiate each of the recommendations within the body of the report. It would also be helpful if they described the intention of the recommendations in terms of the resulting benefit and cost to the ICANN org, and ICANN community, if these particular recommendations were to be implemented."

"The Summary of SSR2 recommendations notes that, 'the SSR2 RT removed any recommendations from this report that did not clearly align with the strategic plan.' ... The SSAC is concerned about the possibility of relevant and useful considerations that impact security and

stability have been removed from this report. Even if they are not recommendations, such material should be noted in this report."

"The SSAC also notes that this section of the report asserts, "All SSR2 RT recommendations align with ICANN org's strategic plan, and so are considered high priority." Yet 4 of the 31 recommendations are marked as medium priority. The SSAC believes it would be helpful for the report to indicate how these priorities were calculated."

"The SSR2 RT might consider rearranging their final report along this [an overarching structured matrix as found in ISO 27001/2 or NIST CSF compliance frameworks] structure, time permitting."

"SSAC is concerned about the extent, cost, sequence, and timeframe of the necessary actions required to implement all of these recommendations. Are there other measures that the SSR2 RT may wish to propose that would give the 135 proposed recommendations a significant prospect of avoiding the same incomplete fate as the 27 outstanding SSR1 recommendations by the time of the next SSR review?"

SSAC makes the following comments on specific recommendations and report sections:

R.1: "It would be helpful for the SSR2 final report to provide a more thorough clarification of the reasons why these SSR1 recommendations are, in SSR2 RT's opinion, not fully implemented."

R.2, 3, 4, 5: "Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, [these recommendations] seem duplicative."

R.3.1: "How does this differ from current ICANN org procedures? What factors led the SSR2 RT to reach this conclusion? Is there an inference that ICANN org has not addressed security issues? The second part of the recommendation relating to promoting security best practices appears to be a distinct issue and merits further clarification. Is ICANN org deficient in this area, and does the SSR2 RT propose actions that would implement their recommendation? Specifically, where are the gaps in capabilities and actions by ICANN org or community in this area? What specific best practices does the SSR2 RT believe should be developed or implemented to address such gaps, and what do they envision as a useful framework to catalog, share, and enhance operational best practices related to a given topic that is relevant to the ICANN community?"

R.3.2: "This recommendation is not practical and cannot be implemented in a reasonable time frame."

R.3.3: "Actions in this recommendation are unclear."

R.3.4: "What aspects of this recommendation differ from ICANN org's current practices?"

R.5: "To what extent do the measures proposed in SSR2 Recommendation 5 differ from current practice within ICANN org? What is the failing in the organisation's policies and procedures that motivate this recommendation?"

Appendix D: “Appendix D enumerates each SSR1 Recommendation and assesses the level of implementation. This section of the report starts by summarizing the SSR2 RT’s understanding of the reasons for the incomplete implementation of the SSR1 Recommendations: ...The SSAC believes that these observations merit further consideration. The SSAC suggests that one way for the report to prompt such consideration is to rephrase these observations as proposals for implementation in the form of Recommendations in the main body of the document.”

R.6: “It would be helpful to understand the context of this recommendation in the light of the existing organisational structure and capabilities of ICANN org.”

R.7: “This is a restatement of Recommendation 5 and it is unclear what objective is achieved through this repetition. The SSAC comments in relation to Recommendation 5 apply here, including the tensions relating to the levels of open disclosure of risk profiles.”

R.8, 9: “The SMART methodology that the SSR2 RT adopted should be used for these recommendations. Specific and clear proposals should be phrased as to how existing BC and DR plans should be revised to meet the criteria described in relevant ISO and ISO/International Electrotechnical Commission (IEC) standards.”

Workstream 3: “It is clear that the nature of abuse in the DNS is so pervasive that elimination is not a realistic objective in the foreseeable future. It would be helpful for the report to note the larger picture of abuse and the necessarily scoped range of actions and consequences that lie within ICANN org’s area of responsibility so that expectations as to the outcomes of the proposed measures are set to achievable levels.”

R.10: “Unless the underlying contractual commitments exist to compel contracted parties to act within clearly defined parameters and responsibilities, then the compliance measures proposed here seem ineffectual. Does the SSR2 RT believe that these contracts are sufficiently prescriptive with respect to behaviours and the residual issue is simply one of enforcement of compliance? As the report notes, “Compliance has few options to enforce the agreements” and the measurements proposed in this recommendation appear to 5 measure ineffectuality of enforcement. Are there measures that could have a beneficial outcome on improving this space?”

R.10.3: Given that the report has noted some challenges relating to enforcement of agreements with contracted parties, it is unclear what the review and the subsequent “recommend the inclusion of requirements” precisely entails. Which party is to perform these reviews? Is it the team envisaged in recommendation 10.2? If not then who would be performing such a review? If so, would these compliance officers possess the skills to be able to, “recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident”? Who is to receive the review’s recommendations? What criteria would be used by this party to assess these recommendations for additional requirements? If requirements are being proposed, where is the contractual foundation to enforce these requirements? Does recommendation 10.3 implicitly refer to recommendation 15, where changes to the contractual conditions are proposed? Some further clarity on these recommendations would be helpful to understand both the detail of the proposed actions and the overall intent of these recommended measures.”

R.11.2: “If the underlying issue is that SSR2 has found evidence that the ICANN Board and ICANN org are not properly processing and acting on the outcomes of other reviews then it should say so explicitly. This recommendation that refers to recommendations from other reviews tends to suggest such a conclusion without actually saying so.”

R.11.3: “What specific actions did the SSR2 RT have in mind? It is challenging to understand the intended objectives of this particular recommendation given the imprecision of the term “encourage community attention”.”

R.11.4: “It appears that the part of this recommendation that refers to SSAC actions is already underway with the formation of a DNS Abuse Work Party within SSAC…The SSR2 RT should consider whether to retain Recommendation 11.4 or simply note in the report that this activity is underway within SSAC.”

R.12.1: “The SSAC largely agrees with the intent of this recommendation, while noting that this measure admits the risk of unintended consequences when considering the generality of the Internet and the diversity of bodies that enforce national regulations. How could ICANN minimize such risks in the context of the implementation of this recommendation?... This general recommendation appears not to take into account the existing activities in this area.”

R.13: “It is unclear if ‘completeness’ here refers to the limited realm of second level domain names in gTLDs. If the intent is a far broader scope of “completeness” including all top-level domains (TLDs) and all labels to an arbitrary depth of delegation, then it would be helpful if the report indicated how such an extension of this activity could take place. Also, the draft report should clearly indicate what is actionable with the specific recommendations, and more precisely, how effectiveness can be measured. Who should get the Domain Abuse Activity Reporting (DAAR) reports, and what should be made public, needs further attention in this recommendation.”

R.14: “Given that ICANN has deliberately distanced itself from any role as a regulator of pricing in this space and holds a position where market forces determine pricing, then what is the context of this analysis and how could such a rigorous quantitative analysis inform the mechanisms of market-based pricing? Further elaboration of the envisaged use of such an analysis would be useful to understand the intended effect of this recommendation. If this recommendation is an oblique reference to heavily discounted prices being applied to bulk name registration practices, then is the underlying abuse issue pricing or bulk registration?”

R.15: “This appears to be a more detailed and clearer restatement of Recommendation 10.3, and in this light Recommendation 10.3 appears to be somewhat unnecessary.”

R.16: “The SSAC has some concerns regarding the propriety and practicality of this recommendation. This proposal may transfer abuse behaviour into those parts of the domain name space that are not directly subject to the same incentives and constraints. Such a program may be extremely difficult to manage and its effectiveness difficult to measure. This

recommendation also proposes a shift of ICANN's role, as ICANN has moved away from a price regulatory role and towards an environment where pricing is a function of market dynamics."

R.17.1: "The SSAC suggests that this recommendation be given a clearer rationale and also should note that any implementation of such a measure should carefully mitigate the inherent risks of undertaking this role of intermediary in abuse reporting."

R.18: "The SSAC is unsure of how this recommendation materially differs from Recommendations 10 and 15."

R.19: "Recommendations 19's consideration to 'update handling of abusive naming' may be an inappropriate designation of responsibility. These recommendations would benefit from an assessment of what falls under ICANN org's remit to enforce, and what efforts ICANN org may be able to facilitate to support a broader community of interest."

R.20.1: "It is useful to understand how various available implementations of DNS name services operate, but it must be remembered that almost any collection of DNS software would by no means include the entirety of the DNS service environment. There are no well understood means of measuring how many end users and services use any particular software bundle, directly or indirectly."

R.20.2: "The SSAC observes that the Root Server System Advisory Committee (RSSAC) Caucus developed such a program, and notes the report from the RSSAC Caucus Work Party states "there was limited use of the testbed after it was completed." It is suggested that the recommendation be revised to recognise the existing activity and to include some proposed measurable outcomes."

R.21: "The interactions of DNS resolvers with respect to multiple instances of authoritative data, and the interactions with cached data held in various recursive resolvers are appreciated in the design of the KSK role. The report's assertion relating to propagation delay is technically fallacious in this context." Additionally, some SSAC reviewers suggest that "the paragraph starting with 'Software and systems process analysis is a research branch of computer science's software engineering ...' and the preceding paragraph beginning with, 'For example, the global DNS Root ..' should be deleted from the draft SSR2 report."

R.21.1: "The SSAC suggests removing this recommendation in its entirety."

R.21.2: "Some SSAC reviewers believe that "his recommendation is simply not implementable in the context of the DNS and the KSK roll…Some SSAC reviewers have suggested that "the SSR2 RT should clarify what work currently underway by ICANN org is not meeting their expectations and identify what work needs to be expanded upon or retooled."

R.21.3: "While this recommendation may be useful, it should not be considered a high priority."

R.22: “The principles espoused in recommendations 22.1 and 22.1 are sound, but their manner of implementation by ICANN should reflect the realities of the at-a-distance relationship between the root server operators and ICANN.”

R.22.3: “This recommendation refers to a “hardening strategy” that is not explained in the draft report.”

R.23: “There are many reasons why secure systems take time to develop and test. … It is unclear why this report is recommending that the process be ‘accelerated’. What issue or issues are being addressed by hastening this particular development? The report does not clearly explain why this acceleration is necessary.”

Root Zone Data and IANA Registries: “The section relating to root zone Data and Internet Assigned Numbers Authority (IANA) Registries seems to contain a mix of considerations relating to the content of 15 the root zone of the DNS, the work of maintaining a collection of protocol parameter registries as a service to the IETF, and the Centralized Zone Data Service (CZDS), which appears to be a service that is a component of the ICANN gTLD DNS function. It may be helpful for the report to independently consider these areas.”

R.24.1: “The scope of this recommendation apparently includes the IETF Protocol Parameter Registry function. Should the agency for whom the function is being performed, namely the IETF, perform a review of ICANN’s performance of execution of the roles described by the Memorandum of Understanding (MoU) between ICANN and the IETF?”

R.25.2: “This again raises the same issue of quoting recommendations from other ICANN supporting organisations and advisory committees. If the reason to reproduce these recommendations in the SSR2 report is because the SSR2 RT has concluded that the ICANN board is not paying due attention to its advisory bodies then it should say so directly. If this is not the case, then what purpose is served by reproducing these recommendations here?”

R.26.3: “This recommendation refers to ‘smoke-testing’. The term is not explained in the draft report.”

Cryptography: “While recommendation 27.1 is general and sufficient as a recommendation, the rationale is too prescriptive”.

R.27.1: “The SSAC agrees with the recommendation that the DPS should provide explicit mention of the possibility of a transition from one digital signature to another”. The SSAC believes that “the explicit references to ECDSA and post-quantum algorithms are unnecessary in this recommendation. The expectation that any such algorithm changes will not degrade security is a prudent expectation, but this recommended action to revise the DPS should remain more generic in nature.”

R.27.2: “The SSAC agrees with this recommendation.”

Workstream 4: “A more logical place for [the “Name Collision”] section of the report would appear to be within Workstream 3’s Review of the Security, Stability and Resilience of the DNS System.”

R.28: ”It is unclear what is being proposed here. The recommendation title in the summary at the front of the report and the recommendation title in the body of the report differ, although the text of the sub-recommendations match. It is also unclear what is meant by ‘Propose a Solution’. This section could benefit from more clarity and context on whether ICANN org should be proposing a solution, to whom the proposal should be presented and how that proposed solution relates to the current NCAP study.”

R.28.1: “In what way does this recommendation materially differ from the existing NCAP study being undertaken under the auspices of SSAC?”

R.28.2: “It is unclear what is being proposed here. Does this recommendation propose the establishment of a new study of name collisions that is to operate in parallel to, but fully independent of, the SSAC NCAP activity? Or is the recommendation proposing a ‘vetting’ of the SSAC NCAP outcomes by some third party or parties that have no financial interest in TLD expansion?”

R.28.3: “What is the intended objective of this recommendation? How would the reported data be used? To what end? The report fails to adequately motivate this recommendation, lack a clear definition of what is intended by ‘community reporting,’ nor give a clear indication of measurable outcomes. In terms of SMART criteria, this recommendation appears to be lacking in terms of specificity, measurability, and relevance.”

R.29: SSAC asks “why is the topic of ‘Privacy’ in Workstream 4 a Future Challenge? This would conventionally be classified as a current topic. Does the SSR2 RT have evidence that ICANN org is not adequately focusing on Privacy and SSR Measurements already? The recommendation implies that the review has taken the position that the level of focus and attention is inadequate, but has not provided any material in the report that substantiates such a conclusion.”

Rationale and Findings on Privacy: “[This section notes] that ‘ICANN org, in having a privacy policy that covers registration information and having Bylaws that requires it enforce its own policies, is in conflict with their statement that ICANN org is not responsible for data protection and privacy.’ This is an unusual interpretation of the ICANN statement, in that the disclaimer is about the general state of privacy on the Internet while the org does have a privacy policy relating to data gathered by the org.”

R.29.1: “It is not clear how this particular recommendation is directly relevant to ICANN. The manner of DNS name resolution between stub and recursive name resolvers on the Internet, and the protocols used to perform such resolution appears to fall outside the scope of ICANN’s activities and authority. Because of this question of direct relevance to ICANN’s scope and mission, this action may be more appropriately included as part of the report’s set of ‘suggestions,’ and listed on the basis of the broader topic of potential actions by ICANN org that would provide value to the community through the provision of assessments of aspects of the larger environment of the domain name space and its evolving use.” The SSAC “is aware of

current activity within both ICANN org and the ICANN community in this space already, including a recently published SSAC study on the implications of DNS over HTTPS and DNS over TLS, and there is some lack of clarity as to how this recommendation differs from current practice."

R.29.2: "The introduction of the concept of DNS 'fragmentation' makes no clear sense in this context. The recommendation should phrase the concern in a different way that avoids the particular term 'fragmentation', or explain the concept of 'fragmentation' in detail."

R.29.3.2: "This recommendation appears to present certain logistical challenges for ICANN org to ensure that ICANN policies and procedures are aligned and in compliance with privacy requirements across all legislative regimes, as the recommendation proposes. Within the review's adopted approach of phrasing SMART recommendations it is unclear how these logistical challenges are to be measured and tracked. The reference to "relevant legislation and regulation" might benefit from a more specific formulation that takes into account the considerable spectrum of variance of national regulations in this space."

R.29.3.3: "The SSAC agrees with the principle behind this recommendation. However, the recommendation appears to imply that ICANN does not have such a policy already, as the recommendation calls for the development of such a policy. To what extent does the ICANN Privacy Policy fall short of the objectives of this recommendation?"

R.29.3.4: "This recommendation lacks clarity and appears to lack measurable outcomes."

R.30.1, 30.1.1, 30.1.2: "[These recommendations] fall short of proposing measures that would facilitate a more engaged interaction between the ICANN community and academic research. The SSR2 RT may wish to consider recommending measures that take a broader approach to this engagement and look at the longer term objectives of such an engagement, instead of the approach taken in this draft report that specifies the content of individual reports."

R.31: "Perhaps the recommendation should be phrased in…more general terms and not specifically refer to DoH."

Further Suggestions: "It would be helpful if the report could clarify the RT's intentions in listing these suggestions. What is the status of these suggestions? Are they formal recommendations? If not, then what is the intended status of the work items that are listed here?"

**FIRST:** FIRST "welcomes the SSR2 recommendations 10, 11 and 13 and looks forward to seeing implementation of these recommendations."

FIRST "suggests, that the following points are taken into consideration:

- ICANN prompt that all registries operate incident response teams
- ICANN promotes and enforces responsible behaviour for registrars
- ICANN works toward a standard to report abuse to registries and registrars
- ICANN develops in a true multistakeholder fashion the development of norms for the domain industry to fight cybercrime."

**RrSG:** RrSG makes the following general comment:

**"**It is not clear how the recommendations below will be carried out. While some recommendations are directed to the ICANN Board or ICANN Org (and within their remit, e.g. audit of Compliance or staffing), many of the recommendations would need to go through the PDP process to avoid having ICANN org creating policy. Those recommendations that include policy elements should be referred to the GNSO Council for further action."

RrSG makes the following comments on specific recommendations:

R.1: "The RrSG agrees with this recommendation."

R.2: "It makes sense for ICANN Org to be certified for key critical certifications like ISO 27001 and 27701 … ICANN Org management, the CEO, and the ICANN Board most fully support such certifications. The ICANN Board should adopt an accountability oversight mechanism for the Board members."

R.3: "The RrSG "doubts that such methods can be applied on a global level without discriminating against certain regions and/or creating high costs for specific contracted parties in certain areas. Modification of the contracts and agreements should not go through a consensus document process. The output from such consensus documents can be considered during arrangements negotiations like any other discussion points during such negotiations."

R.4: "The RrSG supports this recommendation."

R.5: "The RrSG supports this recommendation, which should build upon ICANN Org existing risk management structure."

R.6: "The RrSG agrees that "there should be a position responsible for strategic and tactical security and risk management; it is not clear why this does not already exist. If the function does not already exist, it seems to be a function that fits within the OCTO remit, and so should be part of that team. The RrSG does not consider this specific recommendation as one that requires a PDP; this is something that ICANN Org and the Board can do directly."

R.7, R.9: "These recommendation[s] seems redundant with recommendation 2."

R.8: "With the exception of 8.3, this recommendation seems redundant with recommendation 2, which would require ICANN do to this for ISO certification. The RrSG supports recommendation 8.3."

R.10: "In general, this recommendation is for policy and should go through the ICANN policy process. Regarding the sub recommendations:

- 10.1 - This is already covered by ICANN- Compliance metrics on complaints, Compliance audit, Whois ARS, monitoring by GDD tech team, etc
- 10.2 - This is something Compliance already does. A review team, with limited understanding of the operation and structure, should defer to Compliance to determine how it will best allocate resources.

- 10.3 - It is the position of the RrSG that contract negotiations do not originate from review teams or working groups. That is reserved for ICANN Org, and the RrSG/RySG.
- 10.4 - It is not for a review team to determine the pace of the PDPs or IRTs. There can be unexpected issues that arise (as during the implementation of EPDP Phase 1), and it is better for ICANN to develop and implement policy properly rather than rushing to meet an artificial deadline."

R.12.1: "This is currently being addressed by EPDP Phase 2, and should not be subject to another PDP."

R. 12.2: "There is a pending IRT that is dealing with complex issues. The IRT should be allowed to proceed at its current pace to ensure quality outcome (rather than rushing to meet an artificial deadline)."

R. 13.1: "This data is already being published elsewhere. It is outside of ICANN's scope to aggregate and republish this data. It is also not clear that DAAR is incomplete or ineffective, so additional information is needed to know how the cost for these additional resources outweighs any benefit."

R.13.1.1: "This recommendation should be subject to community consideration before further action."

R.13.1.2: "The recommendation is not very clear what source data for DAAR entails. This data is likely published elsewhere, and it is not ICANN's remit to provide a "clearinghouse" for information that can be obtained elsewhere."

R.13.1.3: If recommendation 13.1.3 is referencing DAAR, then again, these feeds are already available."

R.14: "This was already recommended by CCT. The ICANN board deferred implementing and stated 'questions raised regarding the value of the data' (see https://www.icann.org/en/system/files/files/resolutions-final-cct-recs-scorecard-01mar19-en.pdf). It is not clear what will be accomplished by collecting this information."

R.15: "Contract negotiations should originate through ICANN, the RrSG, and the RySG, rather than a review team. Any recommendations for changes to the RAA or RA are out of scope."

R.15.3.1: "This is most likely not possible because it would violate fundamental rights of data subjects. Furthermore, the correlation between registration data and the effectiveness of actual threat mitigation is unknown."

R.15.3.2: "such research is already possible under many data protection laws. However, current ICANN community processes do not comply with these laws, and as such, the RrSG recommends that the ICANN community focus on how research in a manner that complies with existing laws (rather than making proposals that might violate those laws)."

R.15.4: The RrSG supports "the use of the GNSO to develop ICANN policy."

R.16: “While this recommendation appears to be a good start, it must be subject to a PDP to determine if incentives are a good mechanism to address security threats. As for incentives, they are usually subject to abuse itself and or gaming (and bad actors will figure out a way around it).”

R.16.1.1 and R.16.1.3: “How will ICANN offset the discount (which will result in a lower revenue for ICANN)?”

R.16.1.2: “[This recommendation] will be difficult to implement in light of privacy laws. There are also questions, such as how can registrars verify registrants, what will prevent bad registrars from faking the verification, and does verification mean lower abuse?

R.16.1.4: “It is not clear how [this recommendation] can be tracked. As with other parts of this recommendation, it is subject to gaming/abuse. It could also lead to a new version of frontrunning (e.g. register a domain, track traffic for 25 days, then suspend for ‘abuse’ to get money back if the domain is not generating sufficient parking page revenue or a malicious campaign ends).”

R.16.2: “[This recommendation] is outside of ICANN's remit, and the source of funding for this is not clear (e.g. what would ICANN cancel to pay for this)”

R.17: “It is not clear what are the ‘relevant parties’ in this recommendation. If only registrars and registries, then such a system will likely cost more than any perceived benefit. If it is intended that it would be all inclusive (e.g. P/P providers, hosting providers, etc), it would be outside of ICANN's scope.”

R.18.1: “The RrSG supports that ICANN Compliance should be subject to outside audit.”

R.18.2: “The RrSG notes that these obligations exist in the RAA and Compliance already monitors it.”

R.18.3: “ICANN Compliance already does this (see https://features.icann.org/compliance/dashboard/report-list).”

R.19.1: “Recommendation 19.1 is something that is already shared among commercial and community-driven threat exchanges and are used by many companies for their endpoint protection. It is not for ICANN to aggregate and provide these services for free (as some of them are available for purchase).”

R.19.2: “Recommendation 19.2 is not clear. If a misleading domain names become abusive, then it will be listed in the feeds DAAR uses automatically.”

R.19.3: “Such data needs to be curated and require a Traffic Light Protocol for sharing such information. Furthermore, this requires a clear definition of what is misleading and what can lead to abuse.”

R.19.4: “Recommendation 19.4 should originate from a PDP rather than a review team. Additionally, it is not the place of a review team to initiate RAA or RA negotiation or changes.”

R.20: “it is not clear how this recommendation will be paid for, and what the benefit is over other commercially available solutions.”

R.24: If this recommendation is restricted to the ennumerated items in 24.1, then the RrSG supports this recommendation. If this recommendation is intended to include registrars and registries, then it is not acceptable. As indicated elsewhere, it is not ICANN's role to publicly score the ‘operational status’ of contracted parties.”

R.25: “It is not clear what the concern this recommendation intends to address. Additionally, the term ‘other data’ is very broad and should be narrowed.”

R.29.1, “this appears to be outside of ICANN's remit.”

R 29.2: The RrSG needs additional information about R.29.2, as it is not clear what problem or concern this addressing- those obligations already exist.

R.29.3.1: “Compliance should be allowed to determine its structure and functions without community interference. If this recommendation is adopted, then Compliance would be subject to control by other areas of the ICANN community (and other structures within ICANN as well).”

R29.3.2: “It is the understanding of the RrSG that ICANN already does this, with a focus on all laws that could impact the ICANN community.”

R.29.3.3: “ICANN org should already do this, and this is already covered in the RAA and RA.”

R.29.3.4: “ICANN Compliance already has an audit program. The RrSG need more information regarding R.29.4 as it is not clear what "external DNS PII" refers to.”

R.30: “It is the understanding of the RrSG that ICANN attends a lot of these events already. It is not clear from the draft report how the expense of ensuring attendance and reporting will provide significant benefit, or where ICANN will find the funding for this initiative. Additionally, it is the position of the RrSG that these forums, which have limited (if any) participation of contracted parties, should not be the source for changes to the RAA or RA. There are already existing structures within the ICANN community for the participants of these forums to participate in ICANN's multi-stakeholder model, and this proposed recommendation would circumvent that process.”

R.31: “As with many of the recommendations, this appears to be outside of ICANN's remit, the source of the funds is not clear, and the potential benefits are not defined.”

**RySG:** The RySG makes the following general comments:

“The proposed recommendations would benefit from an explicit statement of the problem that each over-arching recommendation is intended to address.”

“The RySG is concerned about a number of the recommendations that direct the Board or ICANN org to make changes to the Registry Agreement and note that it is not possible for the Board or ICANN org to unilaterally impose new contractual conditions on Contracted Parties. … We would

therefore encourage the Review Team to reconsider the recommendations that direct the Board or ICANN org to make changes to the registry agreement as we do not believe they can be implemented."

"We strongly urge SSR2 to reconsider its prioritization of recommendations and bundle recommendations where they are similar or form a part of a 'package,' and then stack rank the bundles for priorities."

"The RySG would appreciate additional information from the SSR2-RT about how it reached the decision to effectively duplicate the recommendations from a previous Review Team."

"The RySG is also concerned with some of the definitions set out by SSR2 in Appendix A, in particular the definitions of 'security threat' and 'DNS abuse', and note that we do not support the definitions provided. Given SSR2 recommends policy work by the ICANN community to define 'DNS abuse' and 'security threats,' the RySG would ask SSR2 to refrain from creating its own definitions."

Finally, the RySG "does not support the conclusions SSR2 has reached on the next steps, in particular, recommendations for unilateral contract amendments, or pre-determined outcomes of studies or policy work, as we believe both are outside the scope of SSR2's work."

The RySG makes the following comments on specific recommendations:

R.1: "Unless indicated elsewhere in our comments, the RySG supports the implementation of all relevant recommendations."

R.2: "The RySG supports this recommendation."

R.3: "The RySG generally supports this recommendation. However, the RySG notes that "contract changes can be triggered only by Consensus Policy or contract negotiations." Further, the RySG suggests that "the recommendation clarify that the vulnerability disclosure reporting is for the ICANN organization and that ICANN is not a general clearinghouse for vulnerability reports for all contracted parties -those should be directed to the relevant party."

R.4: "The RySG supports this recommendation."

R.5, R.7, R.8, R.9: "The RySG supports [these] recommendation[s] and suggests that [they are] bundled."

R.6: "The RySG does not support this recommendation."

R.10: "We disagree with SSR2's characterization and implication that contractual compliance is so under-enforced or under-resourced that entire new teams need to be hired to deal with specific issues."

R 10.1: "The RySG believes this is out of scope of SSR2."

R10.2: “The RySG does not see the value in specific compliance officers to handle specific contractual compliance issues.”

R10.3: “The RySG believes that this is outside the scope of the SSR2’s work.”

R10.4: “The RySG notes that this recommendation is not made to the appropriate party. A recommendation on a GNSO policy process should be referred to the GNSO Council as the manager of the policy process. Furthermore, it’s outside the scope of a review team to recommend that a PDP wrap up (as it undoubtedly will even without the RT’s recommendation).”

R.11.1: “The RySG does not think it is feasible or realistic for there to be “universally acceptable agreement” on definitions for abuse, SSR, and security threats but is willing to continue its extensive ongoing discussions to try to reach such an agreement.”

R.11.2: “The RySG is unclear about what the SSR2 is asking given R.1 is to implement the remainder of SSR1 recommendations. We do not support the Board unilaterally adopting the definitions established by either the SSR2, the CCT-RT, or the RDS/WHOIS2 Review without full community adoption.”

R.11.3: “The RySG believes “this work is ongoing but objects to the conclusion of this Recommendation as to which definition the Board should adopt. If R.11.3 is to be included as a recommendation, the RySG would only support the text “ICANN Board should encourage community attention to evolving the DNS abuse definition”.

R.11.4: “The RySG believes this is a policy matter and outside the scope of SSR reviews.”

R.12: “The RySG does not support SSR2 making this recommendation given the ongoing EPDP Phase 2 work and questions how this falls within the scope of this review.”

R.13.1: “The RySG notes that “the ONLY entities that can take down domain name abuse are: registries, registrars, hosts, and registrants. There are no third parties that mitigate abuse: only third party tools that analyze data and report on that data.”

R.13.1.1: “The RySG notes that any RO can be the target of abusive activity (through no fault of the RO) and that publishing a list of victims is unlikely to curb actual abuse. We suggest instead focusing on understanding how various RO business models either (or both) prevent or mitigate abuse. DAAR data, without context, is just uncorroborated raw numbers. For instance, a particular RO may experience a 2% abuse rate as a daily average, however that number says nothing about how fast yesterday’s domains were taken down and if the domains on today’s list were also on yesterday’s list.”

R.13.1.2 and R.13.1.3: “Most of the entities that collect and report on behaviors labeled “abuse” by DAAR, do so for a specific, often commercial, purpose. This data is not freely available to the world and ICANN has repeatedly explained that the contracts with the feed providers do not allow them to make the data public. We recognize that many in the community want to see this data for

free and, indeed, so do many ROs. However, simply listing it as a Recommendation will not make it so."

R.13.1.4: "ICANN org has provided a tool and information. It's the community's job to determine if that information should inspire future work."

R.14: "The RySG does not support this recommendation as it is out of SSR2's remit."

R.15: "The SSR RT has no authority to make recommendations to enhance or make changes to the Registry or the Registrar Accreditation Agreements and strongly objects to this set of recommendations."

R.16: "The RySG opposes this recommendation because it's outside the scope of the RT's role."

R.17: "The Registry Agreement requires an email abuse point of contact (POC) on a per-registry basis. Any change to this requirement needs to be the result of a PDP or contract amendment. The RySG further reiterates its concern with the use of the 'abuse' terminology in this recommendation." The RySG "is also unsure why the responses must be publicly searchable, especially considering that they may contain confidential, sensitive or personal information, and that the disclosure of such information could disrupt in-process law enforcement investigations or violate the privacy rights of data subjects."

R.18: "The RySG is unclear why this recommendation is being made."

R.19: "The RySG believes that "this recommendation is outside the scope of SSR2 and does not support it.

R.25.1: "The RySG notes that the current CZDS structure, which currently satisfies the recommendation, was arrived at after much negotiation taking into account the varying concerns of the ICANN community. This negotiated solution should not be overruled by a stroke of the Board's pen."

R.25.2: "The Board has already directed ICANN org to implement these recommendations, so there is no need for the SSR2 to include a recommendation that says the very same thing. This should not be included in the Final Report."

R.28: "The RySG is unclear how this recommendation overlaps with the ongoing NCAP Studies - it's possible that the RT is referring to malicious name collisions at the second level, not inadvertent collisions at the top level. The RySG supports independent studies on malicious name collisions."

R.29: "While the RySG supports ICANN tracking new technology and evolving privacy laws and regulations as part of its overall risk management, the RySG believes that much of this recommendation is out of scope for SSR2."

R.30: "The RySG believes that "tracking academic research on DNS SSR issues should be part of ICANN's risk management strategy."

R.31: “The RySG supports this recommendation.”

**ALAC:** ALAC “notes that in the opinion of the SSR2 RT, many of the recommendations are deemed to be of high priority. Given the current interest in ICANN of prioritizing activities with the implicit effect of not addressing those lower on the list, this could lead to not addressing issues critical to the SSR of the DNS. ... Given the potential for rejection or deferral of the large number of high priority items, the ALAC encourages the review team to strengthen the justification on the high priority items.”

ALAC “has a particular focus on and interest in DNS Abuse. To address this may require contractual changes to facilitate Contractual Compliance action. Such changes require either negotiations with the contracted parties or a PDP. A PDP will take considerable time and the ALAC does not advocate such a path, but rather it is time for ICANN Org and specifically Contractual Compliance to meet with those contracted parties who have shown an interest in DNS Abuse mitigation, and come to an agreement on needed contractual changes, factoring in not only penalties but any incentives that can be reasonably provided to encourage compliance.”

**MM:** MM offers comments on R.16 only:

R.16.1.1: “MarkMonitor supports this novel approach to incentivise rather than chastise. In order to ensure that this is implemented successfully, we need clear definitions of the percentages to identify eligibility and also the identification method should also be defined and explained alongside the reduced fees and/ or discount.”

R.16.1.2: “MarkMonitor also supports this recommendation.”

R.16.1.3: “MarkMonitor supports this offering and appreciates the approach of ensuring that there is an incentive for the registry in addition to registrars.”

R.16.1.4: “MarkMonitor supports this recommendation, however we are aware that the implementation of this scheme may require considerable effort from a policy perspective.”

**WK:** WK suggests that "SSAC, in close cooperation with the ICANN Board and relevant constituencies, should investigate and assess new threats for the security, stability and resilience of the DNS as result of bad behavior of state and non state actors in cyberspace and contribute - within the limit of ICANNs mission - to the intergovernmental and multistakeholder negotiations, which take place within the Open Ended Working Group (OEWG) under the 1st Committee of the UN General Assembly."

WK further suggests “ICANN, within the limits of its mandate and via its Security and Stability Advisory Committee (SSAC), could make constructive contributions with regard to:
a. DNS threat assessment,
b. commenting on relevant norms (as the proposed norm to protect the public core of the Internet),
c. excellent registry and registrar service, based on DNSSEC, to enhance confidence in the DNS and
d. offering technical capacity building for non-technical experts as diplomats.”

**LV:** "Following the publication of: https://www.icann.org/en/system/files/files/ssr2-review-24jan20-en.pdf I note that there is a typo on page 99:DNS-over-HTTP -> DNS-over-HTTPS. I am wondering why https://tools.ietf.org/html/rfc8080 is not mentioned on page 51? Is there an issue with EdDSA for DNSSEC?"

**NCSG:** NCSG "require[s] the SSR2 team to define what the priority levels actually mean. For instance, within what timeframe/deadlines should a priority 'high' recommendation be started, implemented, and reviewed?"

NCSG makes the following comments on specific recommendations:

R.1: "The NCSG considers of vital importance to implement the recommendations from SSR1 that have not been implemented yet, especially Recommendations 9 and 6. In fact, the team found that 26 SSR1 recommendations were not completely implemented and 2 haven't been implemented at all. Therefore, the NCSG invites ICANN board/Org to provide justifications on those matters and take immediate actions to start their implementation in a timely manner. Moreover, the SSR review Team noted that there are four repeating issues. We would like to ask ICANN's Board what actions they will be taking in order to prevent such a situation from occurring again in the future. The affected SSR1 recommendations are the numbers #9, #12, #15, #16, #20, #22, #27, they have now been re-addressed in the recommendations 1 to 5 of the SSR2 that were reviewed by the WS1 team."

R.2: "Recommendation 2 requires ICANN to conduct periodic reviews, audits, etc. of their system's security, stability, and resiliency. We would like to suggest that the review team proposes a specific cycle to conduct the checks. The NCSG suggests that they are conducted on a yearly basis."

R.3: "Recommendation 3 requires ICANN to elaborate the framework and agree with the Metrics and Vulnerability Disclosure. We believe that this process should be done in collaboration with the community represented through the SGs."

R.4: "Recommendation 4 deals with Budget Transparency and Budgeting SSR in the new gTLDs. We suggest that the SSR2 team check how or whether this is related or could be integrated into the ongoing work of the new gTLDs PDP working group."

Workstream 2: "In general, we are in line with all the recommendations (6 to 9) produced by this work stream team."

R.6: "We recommend that the Review team draft a job description that could fit the role. This job description could be appended to the final report."

Workstream 3: "Globally, we have noted that the recommendations made here are pertinent, nevertheless, their measurability would pose a problem … We also caution against the report being used to expand ICANN's remit beyond its current mandate. While DNS abuse is a critical topic, much of the responsibility for structural addressing of this threat rests outside of ICANN's remit."

R.10: “The SSR2 team justifies, elaborates more, analyzes impact and compares what they are recommending here to the current modes of operations. We also note that the recommendation strays into suggesting board action on areas which the review team is not empowered to comment on such as current GNSO policymaking.”

R.11: “As this related to the definition of DNS Abuse, we believe that it is highly important to elaborate more on the methodology and the validation mechanisms.”

R.12: “This recommendation is outside of the review team remit and is already addressed by current ICANN Policymaking in the GNSO and thus should be removed.”

R.13-R.20: “[These recommendations] are all related to DNS Abuse and the DNS operations and are ‘high’ priorities. We recommend that the Review Team proposes a dedicated team, like a cross community Working Group to work on it. We believe that this represents a stronger way/metric to assess the effectiveness of the implementation of those recommendations by a future SSR Team rather than making specific recommendations at this point. We do not fully support the recommendations relating to the opening of DAAR data to private firms for their internal abuse department. This is outside of the role of ICANN and we do not support recommendations related to this topic. On abusive naming we reject the call to replicate the existing systems that were the result of GNSO policy making with regards to trademark confusion and string similarity, again we do not believe that this is within the mandate of the SSR2 RT.”

R.26: “This is vital for the resiliency and stability of the DNS operations. We require the review team to add more measurable actions items to this recommendation. Those should include progression state and deadlines, for instance, 50% of the testing be completed within 5 years, each domain should be tested every 5 years, etc.”

R.31: “We would like to ask the review team to consider the recent report produced by the SSAC, namely the SAC 109, in order to make its recommendations.”

**BD:** The BD offers general observations on the following topics:

- Formulation of draft recommendations
- Prioritization of draft recommendations
- Draft recommendations outside of the Board’s oversight responsibilities:
- Overlap with other community work
- Working towards consensus

The BD makes the following comments on specific recommendations:

R.1: “The Board encourages the SSR2 RT to provide for each SSR1 recommendation an analysis of why it believes that ICANN org’s implementation efforts do not meet the intent of the recommendation, specific details as to what the SSR2 RT sees as the outstanding issues or risks for each SSR1 recommendation, how the SSR2 RT suggests each recommendation should be addressed considering the extensive developments that may have impacted the

recommendations issued nearly eight years ago, and what relevant metrics could be applied to assess implementation in the future."

R.2, R.5, R.7, R.8, R.9: "The Board requests clarification as to what issues or risks exist from the current operational model, how the SSR2 RT recommendations will address them, and what relevant metrics could be applied to assess implementation."

R.6: "The Board encourages the SSR2 RT to provide specific details as to what issues or risks the SSR2 RT has identified with the current operations, how the SSR2 recommendation will address these issues or risks, and what relevant metrics could be applied to assess implementation."

R.10.1: "The Board asks the SSR2 RT to clarify what functionality beyond complaint handling, audits, breach notices, suspensions, and terminations it seeks ICANN Compliance to implement within the scope of the agreements. The Board asks that the SSR2 RT provide greater details on what issues or risks exist from the current operational model, how the SSR2 RT recommendation will address them, and what relevant metrics could be applied to assess implementation."

"Further, it is unclear what is meant by the terms 'performance metrics framework', 'guide level of compliance', and 'other elements that affect abuse, security, and resilience'. The Board suggests that the SSR2 RT provide more detail on the intent of this recommendation to ensure that it is properly considered for implementation. The Board notes that this recommendation may overlap with recommendations from the Initial Report on New gTLD Subsequent Procedures (Section 2.12.3), the Registration Directory Service (RDS)-WHOIS2 Review Final Report and R.4.1, R.4.2, and R.5.1), and CCT Review Team Final Report recommendations (21). The Board requests clarification on the intent of R.10.1 in light of this potential overlap."

R.11.2: "The language of this recommendation presupposes that each of the recommendations are (1) accepted or approved by the ICANN Board; and (2) prioritized by the ICANN community for immediate implementation. The Board notes that it does not believe this to be within scope of the SSR2, and is not aligned with the Bylaws… Additionally, the Board seeks clarification regarding whether this recommendation makes sense in terms of resource deployment in light of the ongoing community discussions regarding the definition of 'DNS abuse'. The Board also seeks clarification of the information the SSR2 RT has to support its position that the definition of abuse has been vetted through the bottom-up multistakeholder process."

R.11.2 and R11.3: "The Board requests clarification as to the intent of these recommendations and whether the SSR2 RT believes it prudent to "implement the SSR-relevant commitments (along with CCT and RDS recommendations) based on current, community vetted abuse definitions, without delay", knowing that the definition may/will evolve."

R.14.1: "The Board notes that this recommendation seems to raise similar questions the Board noted when considering recommendations from the CCT Review Team about collecting pricing data … Given this background, the Board would like to understand whether the SSR2 RT has considered the Board's previous concerns and how that has been factored into its deliberations."

R.15.1: “The Board seeks clarification regarding whether this recommendation would be reasonable in terms of resource deployment in light of the ongoing community discussions regarding the definition of ‘DNS abuse’…Further, as noted above, the Board cannot unilaterally impose new obligations on contracted parties through acceptance of a recommendation from the SSR2 RT.”

R.29.1: “If the SSR2 RT believes additional monitoring and reporting of areas that are within ICANN org’s remit are needed, the Board would encourage the SSR2 RT to provide clear statements of what issues or risks exist from the current operational model, how the SSR2 RT recommendation will address them, and what relevant metrics could be applied to assess implementation.”

R.29.3.2: “The Board encourages the SSR2 RT to consider if [ongoing] work meets the intent of the SSR2 recommendation. If the SSR2 RT believes additional improvements are needed, the Board encourages the SSR2 RT to provide clear statements on what issues or risks exist from the current operational model, how the SSR2 recommendation will address them, and what relevant metrics could be applied to assess implementation.”

R.29.3.3: “The intent of the draft recommendation is unclear to the Board.”

R.29.3.4: “ICANN Contractual Compliance cannot audit something that is not an ICANN contractual requirement…The RA and RAA can only be modified either via a policy development process (PDP) or as a result of contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome.”

R.29.4: “It is unclear to the Board what it means for ICANN to ‘be responsible for external DNS PII’.”

R.30: “The Board supports the work of OCTO and its determination of the needs for data and analysis to inform its work. The Board encourages the SSR2 RT to consider if this work meets the intent of the SSR2 recommendation. If the SSR2 RT believes additional improvements are needed, the Board encourages the SSR2 RT to provide clear statements of what issues or risks exist from the current operational model, how the SSR2 recommendation will address them, and what relevant metrics could be applied to assess implementation. Further, the Board is not clear about the value to the community of a potentially large-scale and costly effort associated with the implementation of this recommendation.”

**WIPO:** WIPO notes broad support for the following recommendations and offers additional supporting comments for each:

- R.12 – R.15
- R.17 – R.19

**ORG:** ORG offers general observations on the following topics:

- Formulation of draft recommendations
- Feasibility of implementation of draft recommendations

- ICANN org considers some recommendations to be already implemented
- Requests for clarification of terms

ORG makes the following comments on specific recommendations:

R.1: “ICANN org encourages the SSR2 RT to provide for each SSR1 recommendation:

- An analysis of why it believes that ICANN org’s implementation efforts do not meet the intent of the recommendation.
- Specific details as to what the SSR2 RT sees as the outstanding issues or risks for each SSR1 recommendation.
- Clarification on how the SSR2 RT suggests each recommendation should be addressed considering the extensive developments that may have impacted the recommendations issued nearly eight years ago.
- Relevant metrics that could be applied to assess implementation in the future.”

R.2: “ICANN org considers this recommendation to already be implemented and asks the SSR2 RT to clarify the observed issue or risk, clearly identify a desired outcome and describe how success will be measured.”

R.3.4: “ICANN org asks the SSR2 RT to clarify which “community-agreed process” this recommendation refers to. ... If the SSR2 RT believes additional improvements are needed, ICANN org asks that the SSR2 RT identify what gaps exist that the Cybersecurity Incident Log does not address.”

R.4.1: “If the SSR2 RT does not consider the current operational model to meet the requirements of SSR2 recommendation 4.1, ICANN org asks the SSR2 RT to provide details as to how it suggests this recommendation should be addressed considering the developments that have occurred since the SSR1 recommendation issued nearly eight years ago, and what relevant metrics could be applied to assess implementation in the future.”

R.5: “ICANN org considers this recommendation already to be implemented and asks the SSR2 RT to clarify the observed issue, clearly identify a desired outcome, and describe how success will be measured.”

R.6: “ICANN org encourages the SSR2 RT to provide specific details as to what issues, risks, or gaps the SSR2 RT has identified with the current operations, how the SSR2 recommendation will address these issues, risks, or gaps, and what relevant metrics could be applied to assess implementation.”

R.7: “ICANN org seeks clarification as to what is meant by “security risk management” as opposed to risk management more generally. The main elements and outcomes of ISO 31000 are included in the ICANN org’s risk management framework. Under the framework, ICANN org uses its own in-house resources to achieve the same outcomes in a fit-for-purpose way. In this regard, ICANN org considers parts of this recommendation to be duplicative of SSR2 Recommendation 5.”

R.8: “ICANN org considers the recommendation regarding disaster recovery already to be implemented … ICANN org supports the recommendation to establish a Continuity Plan for all of ICANN org. Such a Continuity Plan is currently under development as part of the ICANN org’s Risk Management Framework.”

R.9: “ICANN org considers this recommendation already to be implemented. Further, ICANN org encourages the SSR2 RT to include a clear justification as to why it believes the benefits of a third disaster recovery site justifies the costs of such a site.”

R.13: “Work is already underway by ICANN org towards implementation of this recommendation. If the SSR2 RT’s intent is to recommend implementation of something beyond what is in progress with ongoing work, ICANN org encourages the SSR2 RT to provide specific details.”

R.13.1.4: “It is unclear what sort of assistance the SSR2 RT is recommending; ICANN org asks the SSR2 RT to clarify this point. ICANN’s Office of the Chief Technology Officer (OCTO) is particularly interested in ensuring people understand what DAAR data says (and doesn't say). Clarification from the SSR2 RT would be helpful.”

R.13.2: “This appears to be duplicative of 13.1. ICANN org encourages the SSR2 RT to clarify the differences in these two recommendations.”

R.15.1: “ICANN org notes it is unable to unilaterally ‘make SSR requirements mandatory...’. Neither ICANN org nor the Board can unilaterally impose new obligations on contracted parties. The Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board). ... ICANN org therefore encourages the SSR2 RT to consider the ongoing community discussions regarding the definition of "DNS abuse" and how to measure ‘DNS abuse’ through metrics and reporting in finalizing this recommendation, as noted by the Board.”

R.15.3.5: “This recommendation does not include justification as to why ICANN and others would need a vetting process and encourages the SSR2 RT to provide this in its final report. Further, it is not clear to ICANN org which entities the SSR2 RT intends to be vetted or how that vetting can be implemented. With regard to the request in this recommendation to ‘immediately instantiate a requirement’, ICANN org notes that neither it nor the Board can unilaterally impose new obligations on contracted parties. The RA and RAA can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board).”

R.16: “ICANN org notes that “neither it nor the Board can unilaterally impose new obligations on contracted parties. … Further, ICANN org encourages the SSR2 RT to consider and describe what the likely externalities of incentivizing certain behavior might be so that the ICANN org and Board may comprehensively assess the impacts of the implementation of this recommendation.”

R.16.1: “ICANN org encourages the SSR2 RT to consider the ongoing work of the New gTLD Subsequent Procedures PDP Working Group with regard to applicant fees and whether this recommendation may overlap with that work.”

R.16.1.2: As noted in the section “Requests for Clarification of Terms,” ICANN org seeks “clarification of the term ‘verified registrant’. … Additionally, ICANN org encourages the SSR2 RT to consider the potential budgetary implications of a fee reduction.”

R.16.1.3: “ICANN org notes that there are no fees for submitting Registry Services Evaluation Policy requests (RSEPs). Fees only apply if ICANN org identifies potential security or stability concerns and utilizes a Registry Services Technical Evaluation Panel (RSTEP). Is the SSR2 RT referring to RSTEP fees in this recommendation? Further, ICANN org notes concerns regarding the feasibility of implementing this recommendation as pre-approval may not be possible. ICANN org encourages the SSR2 RT to consider in its final recommendation if the Fast Track RSEP Process could be utilized to meet the intended outcome of this recommendation.”

R.16.1.4: “ICANN org repeats its comments above with regard to SSR2 Recommendation 15.1…Additionally, ICANN org has concerns with regard to how this recommendation could be effectively implemented and encourages the SSR2 RT to consider potential issues with gaming and mis-aligned incentives.”

R.17.1: “ICANN org encourages the SSR2 RT to clarify the identified issues or risks that led to this draft recommendation, how the recommended solution will address these issues or risks, the expected impact of implementation, or what relevant metrics could be applied to assess implementation.”

R.18.1: “ICANN org encourages “the SSR2 RT to clarify the identified issues or risks, how the recommended solution will address them, the expected impact of implementation, and what relevant metrics could be applied to assess implementation.”

R.18.2: “ICANN org notes the ICANN Contractual Compliance team does react to complaints and enforces the contractual obligations in the RA and the RAA. ICANN org seeks clarification on what the SSR2 RT means by “systemic abuse,” and the definition used by the SSR2 RT, as well as the meaning of ‘aiding and abetting’ in the context of the recommendation provided by the SSR2 RT. ICANN org would also request clarification regarding which SLA the SSR2 RT is referring to, and why the SSR2 RT feels that this SLA is appropriate in this context.”

R.18.3: “ICANN Contractual Compliance strives to have clear and efficient processes and keep those who make complaints informed and satisfied. If SSR2 RT has data indicating Compliance has not met those goals, ICANN org encourages the SSR2 RT to present the data and develop recommendations that clearly identify ways in which it believes Compliance can better perform their functions to address the deficiencies documented in that data. It is unclear what SLAs SSR2 RT is referring to and with whom those service level agreements would be made. With regards to "maximum public disclosure," ICANN org suggests it would be helpful for the SSR2 RT to

document what information should be disclosed, particularly in light of GDPR-related privacy requirements, to whom, and by what means?"

R.19.2: "Without clear definitions of 'misleading' and/or 'abusive', it is difficult to identify best practices for mitigation and establish criteria that distinguishes between the two… ICANN org notes that in order for an abuse type to be included in DAAR, ICANN org needs a public reputation feed that meets the documented OCTO curation … Further, ICANN org cannot unilaterally develop policy. ICANN org suggests that the SSR2 RT consider directing this element of the recommendation to the Generic Names Supporting Organization (GNSO) Council for review as to whether the recommendation should be considered in a consensus policy development process."

R.20: "ICANN org asks the SSR2 RT to clarify the intent of this recommendation."

R.21: "All advice to the Board is processed via a defined process. ICANN org tracks the implementation of this advice via the Action Request Register (ARR). ICANN org notes that recommendations from any review team cannot circumvent this process and suggests that the SSR2 RT track the status of this advice as it continues to deliberate on Recommendation 21."

R.22.1: "The Governance Working Group (GWG), as defined in RSSAC037, is in the early stages of formation. If the GWG requests assistance from ICANN org in identifying or making available security best practices, we would certainly do so as part of our already existing support for the GWG."

R.22.2: "ICANN org feels that development of Key Performance Indicators (KPIs) to measure root server security best practices should be led by Root Server System Advisory Committee (RSSAC), the GWG, and/or the root server operators themselves."

R.22.3: "It is unclear what problem this recommendation is trying to solve."

R.22.4: "ICANN org has an incident vulnerability disclosure process through the Security and Network Engineering (SaNE) group which operates IMRS. This group is also responsible for ICANN org's digital security. The ICANN org incident disclosure process is therefore applied to the IMRS. Because OCTO defines IMRS strategy and provides and tracks research, including SSR-related research, ICANN org will continue to ensure the SaNE group makes use of the resources available to it. ICANN org encourages the SSR2 RT to consider this work to determine if it addresses the identified issue/risk. If the SSR2 RT's intent is to recommend implementation of something beyond what has already been implemented, ICANN org encourages the SSR2 RT to clarify what issues or risks exist from the current operational model, how the SSR2 RT recommendations will address them, and what relevant metrics could be applied to assess implementation."

R.23.2: "ICANN org requests that the SSR2 RT clarify if it intends this recommendation to require a public comment proceeding whenever IANA makes changes to the RZMS."

R.24.1: “ICANN org encourages the SSR2 RT to consider in its final recommendation if operational status could be grouped by service type and not by unique identifier type.”

R.25.1: “ICANN org encourages the SSR2 RT to “provide examples of ‘unnecessary hurdles’ that requesters are experiencing.”

R.25.2: “ICANN org tracks the implementation of this advice via the Action Request Register (ARR) and suggests that the SSR2 RT may wish to consider the status of this advice as it continues to deliberate on Recommendation 25.2.”

R.26.1: ICANN org requests “the SSR2 to provide more specific language as to what kind of information regarding decisions and dependencies should be made available to help document the EBERO processes.”

R.26.4: ”ICANN org requests clarification as to what issues or risks the SSR2 RT intends to address with this recommendation.”

R.27.1: “ICANN org requests that the SSR2 RT provide a recommendation that more fully elaborates on the essential requirements and conditions for such an algorithm change to be considered and implemented.”

R.27.2: “ICANN org notes that “IANA is consulting with the community on its proposal for how future Root Zone Key Signing Key (KSK) changes will be made. IANA presented this proposal at ICANN66 in Montreal and recently closed a public comment period on it. IANA is reviewing the feedback which will inform the final approach, which will be put into operational practice. ICANN org encourages the SSR2 RT to consider this work as it formulates its final recommendation. Further, ICANN org considers the evaluation of the requirements for a cryptographic algorithm roll to be distinct from evaluating the requirements of future rollovers in general.”

**GAC:** The GAC focuses its comments on the following topics:

General views on the review exercise:

“The GAC welcomes the endorsement of many of the Competition, Consumer Trust and Consumer Choice Review (CCT Review) and Registration Directory Service Review (RDS-WHOIS2 Review) findings and Recommendations. The independent endorsement by three separate cross-community review teams of the same recommendations should be viewed as a strong incentive for swift action. At the same time, the need to repeat identical recommendations or endorsements thereof, shows a mounting concern regarding the state of their implementation.”

“The report could provide a more detailed assessment clarifying the reasons why the SSR1 recommendations are deemed to not have been fully implemented.”

Combatting DNS Abuse:

“The GAC welcomes Recommendation 11 on efforts to implement current community vetted definitions of DNS Abuse without delay and the need to ensure that definitions evolve to meet

continuing threats, in the context of efforts aimed at finding a more effective approach to address DNS Abuse, including with the GAC's support through its advice, comments, and correspondence. Although the GAC shares the overall goal of achieving clarity and consistency with regard to the definition of DNS Abuse and Security Threats, it is not quite clear how the different processes suggested in Recommendations 11.1, 11.3 and 11.4 should interrelate. The GAC therefore invites the Review Team to consider, in view of existing procedures and rules, how this goal can be best achieved."

Evidence-Based Policy Development: The GAC welcomes Recommendations 10, 13, 14 and 19.

Contract Compliance: "The GAC welcomes proposals for specific mechanisms as set out in Recommendations 10.3, 15.1, 15.2 and 16 to incentivize a comprehensive and effective response to DNS Abuse…The GAC also agrees with Recommendation 10.4.'

"The GAC invites the Review Team to consider the articulation between various Recommendations and to clarify how, for example, Recommendations 10.3, 15.1, 15.2, 15.4 and 16, which all propose changes to the contractual framework between ICANN and its Contracted Parties, should work together and be taken forward."

New initiatives: "The GAC welcomes the fact that several recommendations dovetail with priorities the GAC has endorsed for its Public Safety Working Group, such as the inclusion of ccTLDs in DNS Abuse mitigation efforts and the investigation of the security implications of DNS encryption technologies (Recommendations 15, 17, 29 and 31). The GAC invites the Review Team to consider how the work of the PSWG and other parts of the ICANN community could contribute to these efforts."

**IPC:** The IPC concurs with R.1 – R.31 and notes additional details around some of the recommendations. The IPC also makes the following overarching comments:

"The IPC reiterates the importance of ICANN's 'commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates.'

ICANN must fulfill its commitments, including completing the implementation of all relevant SSR1 recommendations which have been left outstanding since 2012.

These commitments are particularly important today as we witness a rise in DNS abuse, which ICANN has not just the opportunity, but responsibility, to address head-on through its SSR commitments."

**Section IV: Analysis of Comments**

*General Disclaimer: This section intends to provide an analysis and evaluation of the comments submitted along with explanations regarding the basis for any recommendations provided within the analysis.*

Commenters did not comment nor were required to provide input on all recommendations. The information in the accompanying spreadsheet was assembled based on comments with a clear indication of support, objection or concern for specific recommendations and was designed to help readers visualize and navigate through level of support. The table is not meant to be a substitute for reviewing the full text of the comments.

In addition to comments on specific recommendations, comments focused on general themes including:

**Prioritization** – A number of respondents asked the SSR2 Review Team to reconsider or further clarify its approach to prioritization, or to provide additional details around its determination

**Outside Bounds of Remit** – A number of respondents noted that numerous recommendations went beyond the remit for the SSR2 review or called for actions outside of the ICANN Bylaws. For example, a number of commenters note that some recommendations direct the Board or ICANN org to make changes to the Registry Agreement, and that the Board or ICANN org cannot unilaterally impose new contractual conditions on Contracted Parties.

**Clarifications** – A number of respondents asked the SSR2 Review Team to provide greater clarity around elements of the recommendations, for example:

- the identified issues or risks
- how the recommended solution will address the issues or risks
- the expected impact of implementation
- what relevant metrics could be applied to assess implementation
- how implementation of the recommendation would differ from existing work that is underway.

**DNS Abuse** – The issue of DNS abuse within the SSR2 Recommendations drew the attention numerous commenters  Beyond the broad concern about the manner to  address DNS Abuse, there is specific concern about the definitions of “security threat”; “misleading” and “DNS abuse” as well as how to measure “DNS abuse” through metrics.  There was also discussion of the need for the GNSO to be engaged, and determine the need for a PDP in areas where ICANN.org cannot make policy.

The SSR2 will undertake an analysis and evaluation of the comments which will be published as an appendix to the SSR2 Final Report.