ICANN Board's Public Comment Submission to the second Security, Stability, and Resiliency (SSR2) Review Team Draft Report

20 March 2020

Dear members of the second Security, Stability, and Resiliency Review Team (SSR2 RT),

The ICANN Board thanks the SSR2 RT for its continued dedication and hard work toward successful completion of the review. The Board appreciates the opportunity to submit a public comment on the SSR2 RT draft report.

The Board acknowledges the progress that the SSR2 RT has made during the course of its work and the response to several engagements and discussions between the SSR2 RT and the SSR2 Board Caucus Group (see for example ICANN60, ICANN64, ICANN66).

This input from the Board is intended to contribute to the refinement of the recommendations and address areas that may benefit from clarification. The Board has general observations on several topics, including: the formulation and prioritization of the draft recommendations; draft recommendations that are outside of the Board's oversight responsibilities; draft recommendations that overlap with other work ongoing in the community; and the SSR2 RT's work toward consensus. The Board also includes in this comment some other inputs on specific draft recommendations, as noted below. The Board may provide the SSR2 RT with additional input as the team's work progresses. We will strive to provide such input in a timely fashion to inform SSR2 RT work in consideration of your timeline.

General Observations

Formulation of draft recommendations

As part of its deliberations on review team recommendations, it is helpful for the Board to have an understanding of the particular issues or risks that each recommendation intends to address. The Board's draft proposal for resourcing and prioritization of community recommendations developed with input from leadership of all specific review teams, notes that an effective recommendation should address an observed issue that has significant consequences for ICANN as a whole. Clear articulation of the observed issue gives insight into the intent of the recommendation and the justification for why it should be adopted. With this in mind, the Board notes that a number of the SSR2 RT's recommendations, as currently drafted, do not clearly define the identified issues or risks, the rationale for the recommended solutions, the expected impact of implementation, or what relevant metrics could be applied to assess implementation. Some examples as outlined in this comment include SSR2 RT recommendations 1, 2, 5, 6, 7, 8, 9, 10.1 and 29.

Further, the Board notes that it is unclear what information and analysis the SSR2 RT considered when forming its recommendations. These elements of each recommendation should be well understood by all for the Board to properly consider the recommendations and make appropriate instructions to ICANN org and/or community. Section 4.1 of the Operating Standards for Specific Reviews (Operating Standards) provides guidance on how to formulate concrete fact-based problem statements and clear definition of what the desired outcome will look like,

including how implementation should be evaluated by the community and the next review team, and the impact of implementation on ICANN resources and on the ICANN community workload. While the Operating Standards were adopted after the SSR2 RT started its work, the Board encourages the SSR2 RT to consider the Operating Standards, developed in consultation with the community as mandated by the ICANN Bylaws Section 4.6 when compiling its final report. The draft proposal referenced above also provides some suggestions toward effective recommendations and the Board urges SSR2 RT to follow these practical suggestions to improve the clarity and usefulness of its recommendations.

Prioritization of draft recommendations

The Board appreciates the SSR2 RT's efforts to prioritize its recommendations and acknowledges the SSR2 RT is seeking feedback on this work. The Board notes that the SSR2 RT has drafted 31 recommendations, many of which have subcomponents, resulting in more than 100 recommendations in total. The SSR2 RT has prioritized those recommendations as 'high' or 'medium'. While in no way criticizing the approach the SSR2 RT took to establish the priorities they assigned, the Board encourages the SSR2 RT to consider relevant factors such as dependencies and relationships with other community work, determination of effort, as compared to expected impact of implementation work, or degree of complexity, among others, in order to categorize each recommendation as 'high priority', 'medium priority', or 'low priority'. This analytical and tiered approach will provide a more useful guideline for planning timely implementation of the recommendations.

The Board notes that there are nearly 300 recommendations issued by specific reviews (not including the third Accountability and Transparency Review (ATRT3) and SSR2 recommendations), organizational reviews, and the CCWG-Accountability's WS2 that are either pending consideration by the Board or are awaiting implementation following Board action. The ICANN community, the ATRT3, and the ICANN Board have been discussing the large number of recommendations and are seeking workable solutions for prioritizing recommendations that take into account limited time and resources of all parties involved (see "Resourcing and Prioritization of Community Recommendations: Draft Proposal for Community Discussions", Chairman's Blog "Enhancing and Streamlining ICANN's Reviews: Issues, Approaches, and Next Steps", and ATRT3 Draft Report Public Comment proceeding).

Draft recommendations outside of the Board's oversight responsibilities

The Board notes that a number of the SSR2 RT's recommendations currently directed to the Board are outside of the Board's oversight responsibilities. For example, the Board cannot unilaterally impose new obligations on contracted parties through acceptance of a recommendation from the SSR2 RT. The Registry Agreement and Registrar Accreditation Agreement (RAA) can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome. The Board suggests that the SSR2 RT consider directing these recommendations either to ICANN org for inclusion in a future round of voluntary contract negotiations and/or to the GNSO Council for review as to whether the recommendation should

be considered in a consensus policy development process. Some examples of recommendations to which these observations apply include SSR2 RT recommendations 11.1, 12, 15, 18.2, 19, and 29. Further, the Board suggests that the SSR2 RT consider directing SSR2 RT recommendation 22.1 to the Root Server System Governance Working Group which has recently been formed.

Overlap with other community work

The Board notes that there is overlap between a number of the SSR2 recommendations and other work ongoing in the community, whether from review teams, working groups, or ICANN org efforts. To the extent SSR2 recommendations have dependencies with other multistakeholder processes across ICANN, it is important that the Board maintain and confirm its role, as specified in the Bylaws. Where the SSR2 RT is aware of such overlap, the Board encourages the SSR2 RT to suggest that its recommendations be consolidated into or passed through to ongoing work conducted by the community, or to clarify how the intent of the SSR2 RT's recommendation is to implement something beyond what is already in progress. The Board suggests that clarification regarding the SSR2 RT's expectations for these recommendations may also assist with the SSR2 RT's prioritization efforts, in line with the Board's comment above. Some examples of overlap with community work include:

- *SSR2 recommendations 3, 10, 11, 13, 14, 16.1.1, 17, 19, 24, 28, and 30:* These recommendations may overlap with ongoing work related to the Open Data Program, Competition, Consumer Trust, and Consumer Choice Review Team (CCT) recommendations, Global Domains Division engagement functions, and/or Name Collision Analysis Project (NCAP).
- *SSR2 recommendation 10.3 and 26:* These recommendations may overlap with recommendations from the Initial Report on the New gTLD Subsequent Procedures on Registry System Testing (Section 2.11.1) and Registrant Protections (2.7.2).
- *SSR2 recommendation 29.3.2:* This recommendation may overlap with ongoing work being conducted by ICANN org regarding the tracking of legislation.

Working toward consensus

The Board understands that the SSR2 RT has not reached consensus on the recommendations presented for comment and notes that this point is not clearly articulated in the draft report. The Board acknowledges that the SSR2 RT has committed in its Terms of Reference (section "Decision Making" on pages 5-6) to striving to make decisions by consensus and to include minority views in its reports where the SSR2 RT is unable to achieve consensus with respect to any recommendation. The Board reminds the SSR2 RT that the degree of consensus or agreement reached by the SSR2 RT on each recommendation should be clearly noted in the SSR2 RT's final report, in accordance with the ICANN Bylaws Section 4.6. The Board notes that the Operating Standards offer guidance on decision-making procedures in section 3.11.

Observations on Specific Recommendations

ICANN Board's Public Comment Submission to the second Security, Stability, and Resiliency (SSR2) Review Team Draft Report

20 March 2020

SSR2 Recommendation 1: The SSR2 RT strongly recommends that the ICANN Board and ICANN org complete the implementation of the SSR1 Recommendations.

The Board notes that ICANN org delivered to the SSR2 RT a detailed and factual report of the implementation steps it has completed for each SSR1 recommendation (see briefing materials). These materials include status of work, links to substantiating details, and notations of limitations encountered in implementation. Reference was provided when a recommendation was overtaken by other work. ICANN org's reporting on the status of work does not address the more subjective evaluation performed by the SSR2 RT, which at times addresses whether the described implementation is to be deemed effective, or if there might have been other paths to implementation that the SSR2 RT might have preferred.

To that end 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.

SSR2 Recommendations 2, 5, 7, 8 and 9

SSR2 recommendations 2, 5, 7, 8 and 9 deal with certifications, security audits, risk framework, security risk management framework, business continuity plans, and disaster recovery for ICANN and PTI. In connection with these recommendations addressing various aspects of risk management within ICANN org, 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.

The Board understands that ICANN org has provided detailed information to the SSR2 RT with regard to risk management in the org. For example, ICANN org has responded to questions on this topic from the SSR2 RT and has noted its centralized Risk Management Framework, and established disaster recovery and continuity plans for systems covering both ICANN org and IANA functions. Documents regarding disaster recovery and continuity planning are confidential and are not published for security reasons.

The Board receives regular updates from ICANN org and has oversight responsibility for ensuring that these programs are in place. The Risk Committee of the Board is responsible for the assessment and oversight of ICANN implemented policies designed to manage ICANN's risk profile, including the establishment and implementation of standards, controls, limits and guidelines related to risk assessment and risk management. The Board considers the policies, plans, and programs that ICANN org has in place to be appropriate and therefore considers these recommendations already to be operational and part of the Board's regular oversight

responsibility. If the SSR2 RT does not agree with the Board's assessment, the Board requests the recommendation explain what is missing, the risks associated, how SSR2 RT suggests those risks should be addressed, and what relevant metrics could be applied to assess implementation.

SSR2 Recommendation 6: Create a Position Responsible for Both Strategic and Tactical Security and Risk Management

As noted above, as a general observation on the formulation of draft recommendations, 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.

SSR2 Recommendation 10.1: Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review.

The SSR2 RT states in its findings with respect to recommendation 10 that, *"ICANN Compliance has not publicly requested specific changes to the RAA or RA, nor has it incorporated functionality to monitor service levels, penalties, or circumstances that warrant suspension of a registrar's or registry's privilege to process new registrations"* (page 33 of the draft report). ICANN org operates a Service Level Agreement Monitoring (SLAM) system and Compliance is notified when SLAs are violated. The Board notes that ICANN org carries out voluntary contract negotiations with contracted parties. The Board also notes that as part of the bottom-up multistakeholder process, the ICANN community can develop policies to address issues of concern to the ICANN ecosystem. Further, 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 recommendations (4.1, 4.2, and 5.1), and CCT Review Team Final Report recommendations (21). The Board requests clarification on the intent of recommendation 10.1 in light of this potential overlap.

ICANN Board's Public Comment Submission to the second Security, Stability, and Resiliency (SSR2) Review Team Draft Report

20 March 2020

SSR2 Recommendation 11.2: ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay.

The Board notes that the CCT Final Report and recommendations are being considered and implemented as appropriate as already discussed with the community. The Board took action on the RDS Final Report and recommendations in line with the Bylaws requirements. 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.

SSR2 Recommendation 11.3: ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of "security threat"—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique and for Specification 11), and addressed in international conventions such as the Convention on Cybercrime and its related "Explanatory Notes"—to use in conjunction with ICANN org's DNS Abuse definition.

In reviewing recommendations 11.2 and 11.3 together, 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.

Furthermore, the Board seeks clarification as to how the SSR2 RT would assess effective implementation of this recommendation. It is not clear what the measure of success would be given that the Board cannot mandate the community to reach agreement on the definition of "DNS abuse". It is also not clear what the SSR2 RT intends for the Board to do in "adopting" a definition. The Board believes that the issue is not about "abuse definition", but about what kind of DNS abuse is within ICANN's remit.

SSR2 Recommendation 14.1: ICANN org should collect, analyze, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse.

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 (see page 4 of the scorecard with regard to CCT recommendations 3 and 4). With regard to the relevant CCT Review Team recommendations, the Board placed them in "Pending" status, and directed ICANN org, through engagement of a third party, to conduct an analysis to identify what types of data would be relevant in examining the potential impacts on competition and, whether that data is available, and how it could be collected in order to benefit the work of future CCT Review Teams. The Board stated that this analysis would inform the Board's decision on next steps and whether the recommendations could be adopted.

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.

SSR2 Recommendation 15.1: ICANN org should, make SSR requirements mandatory on contract or baseline agreement renewal in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, These contract requirements should include provisions that establish thresholds of abuse (e.g., 3% of all registrations) that would automatically trigger compliance inquiries, with a higher threshold (e.g., 10% of all registrations) at which ICANN org considers registrars and registries to be in default of their agreements. The CCT Review also recommended this approach.

As noted with regard to SSR2 recommendation 11.2, 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. The Registry Agreement and Registrar Accreditation Agreement (RAA) can be modified either via a consensus policy development process or as a result of voluntary contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome.

SSR2 Recommendation 29.1: ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS).

The Board supports the work already underway in this area by the ICANN Office of the Chief Technology Officer (OCTO) and the Technical Committee of the Board. See for example the October 2019 report, 'Local and Internet Policy Implications of Encrypted DNS'. The Board also notes that the ICANN Security and Stability Advisory Committee (SSAC) recently published a report on the implications of DNS over HTTPS and DNS over TLS (see SAC109). The Board believes that this work addresses the recommendation proposed by SSR2 RT. 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.

SSR2 Recommendation 29.3.2: Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation.

The Board notes that ICANN org regularly publishes reports on global legislative and regulatory developments (including privacy legislation) to identify legislative efforts across the globe early-on, to raise awareness within ICANN, and allow for potential impacts to be considered. Additionally, the Board recently took action on the RDS-WHOIS2 Final Report and recommendations, including two recommendations that call for monitoring of legislative and policy development around the world - R1.1 and R1.2. The Board approved these recommendations, noting that corresponding activities are already part of ICANN's plans. 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 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.

SSR2 Recommendation 29.3.3: Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented.

The intent of the draft recommendation is unclear to the Board. As stated in the ICANN Bylaws, in performing its mission, ICANN must "[carry] out its activities in conformity with relevant principles of international law and international conventions and applicable local law…." With this in mind, is the intent of the recommendation for the Generic Names Supporting Organization (GNSO) to initiate a consensus policy development process to develop a privacy policy for the protection of personally identifying information in registration data? Or, is the intent of the recommendation to direct that ICANN org have a privacy policy for the personal data that it processes as part of its operations? If the latter, the Board notes that ICANN org has a Privacy Policy in place, which is available here: https://www.icann.org/privacy/policy. The Board encourages the SSR2 RT to consider if this work meets the intent of the recommendation. If this is not the intent of the SSR2 RT, the Board encourages 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.

SSR2 Recommendation 29.3.4: Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches.

The Board notes that since 1999, the Registrar Accreditation Agreement has included certain data protection obligations, including requirements that registrars provide notice to registrants about the purposes for which personal data is collected, the intended recipients of the data, and how the registrant can access and, if necessary, rectify data held about them. These requirements, like other requirements in the agreement, are subject to audit. Aside from those requirements, ICANN org does not specifically require registrars to have "privacy policies". ICANN Contractual Compliance cannot audit something that is not an ICANN contractual requirement.

Additionally, there is a difference between having a privacy policy and addressing data/privacy breaches. As the Board stated in its recent action on the RDS-WHOIS2 Review Final Report and recommendations, specifically on recommendation SG.1, "*the Board notes there are provisions already in the Registrar Accreditation Agreement (RAA) regarding notification to ICANN on certain security breaches, and that the Registry Agreement (RA) does not currently require registry operators to inform ICANN in the event of security breaches. As contemplated by the RDS-WHOIS2 RT, these contracts would have to be amended. However, the Board cannot unilaterally impose new obligations on contracted parties through acceptance of a recommendation from the RDS-WHOIS2 RT. 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.*"

SSR2 Recommendation 29.4: ICANN org's DPO should also be responsible for external DNS PII. The DPO should provide guidance to managers and stakeholders regarding responsibilities and procedures and monitor and report on relevant technical developments.

It is unclear to the Board what it means for ICANN to "be responsible for external DNS PII." As the SSR2 RT may be aware, the ICANN org Chief Data Protection Officer (CDPO) focuses on ICANN organization-level data, to ensure ICANN's internal data protection and privacy program is compliant and up to date. The CDPO also advises ICANN org on how best to handle and process personal information ICANN org collects as it continues to fulfill its core commitments and obligations and provide both internal and external services in a compliant manner.

The organization-level role is not intended to cover the use of data by Registrars and Registries under ICANN's contracts, which is part of the broader discussion relating to the European General Data Protection Regulation (GDPR) and the impact of these regulations on ICANN contracts. The impact of GDPR regulations on ICANN contracts is a discussion taking place in the broader ICANN community as part of consensus policy discussions. The Board notes that it is the responsibility of every entity that agrees to collect, maintain, or process data to ensure that

their data protection responsibilities under applicable laws are fulfilled. ICANN org cannot legally serve as an external legal advisor to its contracted parties on this matter. Additional clarity on the intent of the recommendation would be helpful.

SSR2 Recommendation 30: Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates.

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.

Next Steps

The Board notes that ICANN org is completing its analysis of the SSR2 draft report and intends to submit a separate comment on operational matters.

The Board looks forward to receiving the final report of the SSR2 RT in due course. Once available, the Board will move forward with the process outlined in the Bylaws for considering the final report. Please keep us informed of your progress and let us know how we can support your work. Again, the Board thanks the SSR2 RT for its dedication to this important review.

Sincerely,

Maarten Botterman
Chair, ICANN Board of Directors