ICANN Organization Public Comment Submission to the second Security, Stability, and Resiliency (SSR2) Review Team Draft Report
27 March 2020

Dear members of the second Security, Stability, and Resiliency Review Team,

ICANN organization appreciates the opportunity to submit a public comment on the second Security, Stability, and Resiliency Review Team (SSR2 RT) draft report. Having engaged with the SSR2 RT throughout the course of the review team's work, starting in March 2017, via briefings, background materials, responses to information requests, and direct interactions, ICANN org notes the extensive work that the SSR2 has undertaken.

This comment focuses on the operational elements of the SSR2 RT draft report on which ICANN org seeks clarification and areas that could benefit from refinement to ensure the SSR2 RT produces effective recommendations. ICANN org acknowledges that the SSR2 RT is already in the process of making proposed modifications to a number of its recommendations and reiterates that this comment addresses the recommendations as stated in the draft report.

This comment highlights several overarching observations - formulation of draft recommendations, feasibility of implementation of draft recommendations, recommendations that ICANN org considers to be implemented already, etc. Following these overarching observations, we include detailed comments and observations on specific recommendations.

Formulation of draft recommendations

ICANN org reiterates the Board's comment that it is helpful for the ICANN org, Board, and community to have an understanding of the particular issues or risks that each recommendation intends to address. A number of SSR2 recommendations, as currently drafted, do not clearly define the identified issues or risks, how the recommended solution will address the issues or risks, the expected impact of implementation, or what relevant metrics could be applied to assess implementation (for example, SSR2 recommendations 1, 2, 5, 6, 7, 8, 9, 15.3.4, 15.3.5, 18, 19.1, 19.2, 23.1, 26.2, and 29.2). ICANN org encourages the SSR2 RT to clarify these elements of each recommendation for the Board to properly consider the recommendations and make appropriate instructions to the ICANN org and/or community.

Feasibility of implementation of draft recommendations

ICANN org also welcomes this opportunity to provide feedback on the operational feasibility of implementation of the SSR2 RT recommendations. This comment addresses a number of recommendations that, as currently drafted, may not be feasible for ICANN org to implement because the recommendation would appear to require

ICANN org to act outside of its mission and scope (for example, SSR2 recommendations 15, 16, 19.2), or the expected impact of implementation is not clearly defined (for example, SSR2 recommendations 5, 6, 18, 20). ICANN org encourages the SSR2 RT to further engage with ICANN org subject matter experts to ensure feasibility and usefulness of its recommendations.

ICANN org considers some recommendations to already be implemented

Work is already underway by ICANN org, community, and/or Board to address issues identified by SSR2 RT and the subject of some of these recommendations. It is not clear if the SSR2 RT considered the briefings, background material, or responses to information requests about work underway when formulating its recommendations. 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. Some examples of recommendations that ICANN org considers to already be implemented include SSR2 Recommendations 2, 3.4, 4.1, 5, 7, 8, 9, 22.4, 25.2. Work is already underway to address issues identified by SSR2 Recommendations 13 and 21.

Requests for clarification of terms

A number of SSR2 RT recommendations include specific terms that ICANN org may not fully understand in the context of the SSR2 recommendation. To ensure that the identified issues or risks, the recommended solutions, and the expected impact of implementation of the recommendation are clearly defined and understood by all, ICANN org encourages the SSR2 RT to define the following terms in the context of the recommendation:

- **SSR Recommendation 3.2:** “SSR-related best practices”
- **SSR2 Recommendation 7:** “security risk management”
- **SSR2 Recommendation 13.1.2:** “source data”
- **SSR2 Recommendation 16.1:** “commercial providers”
- **SSR2 Recommendation 16.1.2**: “verified registrant”
- **SSR2 Recommendation 17.1:** “abuse report”
- **SSR2 Recommendation 18.2:** “as defined by the SLA”
- **SSR2 Recommendation 19.1:** “misleading naming”
- **SSR2 Recommendation 19.2:** “misleading naming” and “abusive naming”
- **SSR2 Recommendation 26.3:** “smoke testing”

- **SSR2 Recommendation 29.2:** "with these"

Observations on Specific Recommendations

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

ICANN org reiterates the Board's comment on SSR2 Recommendation 1 which 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). 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.

SSR2 Recommendation 2: SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications

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. As ICANN org has noted in response to questions on this topic from the SSR2 Review Team, ICANN org has performed annual cybersecurity framework (CSF) assessments based on the CIS20 Cybersecurity Framework from 2014 to 2018, subsequently moving to the NIST Cybersecurity Framework. In 2018, ICANN org also changed to bi-annual assessments because ICANN org's information security capabilities have matured to the point that the year-to-year changes are relatively small. The benchmarking assessments are conducted by a consulting firm with expertise in such assessments. ICANN org provides regular reports to the Board on the CSF assessments and cybersecurity generally (see for example the Board Technical Committee November 2019 meeting minutes).

In addition, two annual information security audits are performed related to the IANA functions. The IANA department has been performing SOC3 audits on the Root Zone Key Signing Key Operator System since 2010, and SOC2 audits on the Registry Assignment and Maintenance System since 2013. Those audits are performed by external auditors and the reports of those audits are available at https://www.iana.org/about/audits.

SSR2 Recommendation 3.4: ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community-agreed process and include anonymized metrics.

ICANN org asks the SSR2 RT to clarify which “community-agreed process” this recommendation refers to. Any disclosures we make in terms of an incident is based on ICANN org’s own incident reporting process. ICANN org maintains the Cybersecurity Incident Log at https://www.icann.org/cybersecurityincidentlog. In general, ICANN org will disclose major security vulnerabilities and resulting incidents that cause significant risk to the security of ICANN's systems, or to the rights and interests of data subjects, or otherwise require disclosure under applicable legal requirements.

ICANN org’s coordinated vulnerability disclosure process is available at https://www.icann.org/vulnerabilities.

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.

SSR2 Recommendation 4.1: Where possible (contractually) and reasonable in terms of effort (i.e., over 10% of the activity described in the budget line item), ICANN should be more transparent with the budget for parts of ICANN org related to implementing the Identifier Systems Security, Stability, and Resiliency (IS-SSR) Framework and performing SSR-related functions, including those associated with the introduction of new gTLDs.

ICANN org notes that the SSR Framework is no longer produced, as has been previously noted to the SSR2 RT (see most recently, for example, ICANN org’s discussion with the SSR2 RT on 8 January 2020). SSR-related elements are included in the ICANN Five Year Strategic and Operating Plans, and the Annual Operating Plan and Budget. In an effort to address SSR1 Recommendations 20, 21, and 22, in Fiscal

Year 2018 (FY18) ICANN org created the Operating Plan of SSR Related Activities to be used as a mechanism to provide more detailed public information on SSR related budgets and expenditures across multiple ICANN departments. 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.

SSR2 Recommendation 5: SSR1 Recommendation 27 - Risk Management

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.

ICANN org has a centralized risk management function. The risk management framework and the plans for developing risk management capabilities were presented to the SSR2 team in a face-to-face meeting in October 2018 by ICANN org's VP of Risk Management, and Chief Finance Officer.

As noted by the Board, the Risk Committee of the Board (BRC) 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 receives regular updates from ICANN org and has oversight responsibility for ensuring that these programs are in place. Minutes of the September 2019 BRC meeting refer to the "Organization Risk Register", which reflects the organization-wide risk as identified and measured by the risk management function, in cooperation with all functions and regions across ICANN org. Other references to the Organization Risk Register in 2019 alone can be found in the August 2019 and February 2019 BRC meeting minutes.

Considering that many risks are vulnerabilities to ICANN org and the ICANN community, making detailed information about specific risks public may itself be a risk and thus, publication of those risks is limited. Related to this recommendation, during this fiscal year, ICANN org will provide a proposal to the Board for a Risk Appetite Statement which, once adopted by the Board, will be shared with the ICANN community.

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

Because of the diversity of the types of security challenges (internal systems, physical, staff safety, external to the continued function of the identifiers in which ICANN manages), ICANN org made the conscious decision to distribute the various security functions to the relevant functional areas within the organization. These functional teams work closely not only with one another but also with the BRC which, as noted above, provides oversight as to the risk based functions for which ICANN org is responsible.

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.

SSR2 Recommendation 7: Further Develop a Security Risk Management Framework

As noted above, 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.

As noted above, the risk management framework and the plans for developing risk management capabilities were presented to the SSR2 team in a face-to-face meeting in October 2018. Minutes of the September 2019 BRC meeting refer to the “Organization Risk Register” which reflects the organization-wide risk as identified and measured by the risk management function, in cooperation with all functions and regions across ICANN org.

SSR2 Recommendation 8: Establish a Business Continuity Plan Based on ISO 22301

This recommendation mentions Disaster Recovery and Business Continuity Planning. ICANN org considers the recommendation regarding disaster recovery already to be implemented. ICANN org has established disaster recovery and continuity plans for systems for ICANN org and IANA functions. Due to potential risks of providing attackers with information to facilitate attack, documents regarding disaster recovery and continuity planning are confidential. The Board has oversight responsibility for ensuring that these programs are in place.

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.

SSR2 Recommendation 9: Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented

As noted with regard to SSR2 Recommendation 8, 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.

SSR2 Recommendation 13: Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program

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. ICANN org encourages the SSR2 RT to consider the following work with regard to SSR2 recommendation 13:

- *SSR2 Recommendation 13.1:* ICANN org solicits input from all stakeholders on how to improve DAAR on a regular basis, including via daar@icann.org and the "DNS abuse measurements" mailing list.
- *SSR2 Recommendation 13.1.1:* ICANN org is in discussions with relevant stakeholders as to how best to provide data to inform policy discussions.
- *SSR2 Recommendation 13.1.2*: Publishable DAAR-related data is already slated to be included in the Open Data Platform.
- *SSR2 recommendation 13.1.3:* With the inclusion of DAAR data into the Open Data Platform, this recommendation will be implemented.
- *SSR2 Recommendation 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.

- *SSR2 Recommendation 13.2*: This appears to be duplicative of 13.1. ICANN org encourages the SSR2 RT to clarify the differences in these two recommendations.

ICANN org continues to encourage the SSR2 RT to engage with relevant ICANN org subject matter experts to ensure that recommendations related to DAAR issued in the SSR2 RT's final report are within the role and function of the project.

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.

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). However, there is still a lack of agreement within the community with regard to defining and measuring what constitutes "DNS abuse". Having common definitions of abuse or security threats first would be helpful for effectively framing a policy development process or voluntary contract negotiations that are intended to develop requirements that penalize or incentivize behavior to mitigate abuse. The development of any such requirements would likely also need to consider how to account for false or inaccurate reports of "DNS abuse" against the contracted parties. 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.

SSR2 Recommendation 15.3.5: Immediately instantiate a requirement for the RDAP services of contracted parties to white-list ICANN org address space and establish a process for vetting other entities that RDAP services of contracted parties will whitelist for non-rate-limited access.

ICANN org notes that 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).

SSR2 Recommendation 16: ICANN org should incentivize the mitigation of abuse and security threats making the following changes to contracts[.]

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).

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.

SSR2 Recommendation 16.1: Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount).

As noted in the section “Requests for Clarification of Terms,” ICANN seeks clarification regarding the term “commercial providers”. ICANN org also notes that this recommendation may overlap with ongoing work related to the Competition, Consumer Trust, and Consumer Choice Review Team (CCT RT) recommendations. The Board passed through CCT recommendation 12 regarding incentives to the New gTLD Subsequent Procedures PDP Working Group (see page 2 of the scorecard). 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.

SSR2 Recommendation 16.1.2: Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.

As noted in the section "Requests for Clarification of Terms," ICANN org seeks clarification of the term "verified registrant". Is the SSR2 RT referring to potential activities to "verify" the identity of a registrant? If this is the case, ICANN org encourages the SSR2 RT to consider this recommendation in light of ongoing discussions and work related to the European General Data Protection Regulation (GDPR), including the feasibility of conducting such activities in light of GDPR, and the impact on ICANN contracts. Specifically, depending on what the SSR2 RT means by "verified registrant", conducting verification activities could have potential implications for ongoing discussions related to access to non-public registration data as well as controllership. That is, who does the SSR2 RT envision would be conducting the verification and managing the data related to verified registrants? Additionally, ICANN org encourages the SSR2 RT to consider the potential budgetary implications of a fee reduction.

SSR2 Recommendation 16.1.3: Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant.

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.

SSR2 Recommendation 16.1.4: Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered).

ICANN org repeats its comments above with regard to SSR2 Recommendation 15.1, namely that consideration should be given to the ongoing community discussions regarding the definition of "DNS abuse" as well as metrics/reporting for abuse. 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. For example, contracted parties might have less incentive to guard against the creation of domains intended for misuse or might in some cases even profit from their creation if they end up being "free" of ICANN transaction fees.

SSR2 Recommendation 16.2: Given all parties (ICANN org, contracted parties, and other critical stakeholders such as Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers, and the contracted parties) must understand how to accurately measure, track, detect, and identify DNS abuse, ICANN org should institutionalize training and certifications all parties in areas identified by DAAR and other sources on the common methods of abuse [citation to be added] and how to establish appropriate mitigation efforts. Training should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Quarterly/Yearly public reports on complaints and actions; and analysis.

ICANN notes that both in Recommendation 15.4 and 16.2, the SSR2 RT recommends that ICANN org "institutionalize training and certifications." ICANN org requests clarification regarding the SSR2 RT's expectations for training and certifications (i.e., types, methods) as well as the intended meaning of "institutionalize." Is the SSR2 RT requesting that general training courses be offered, for example through ICANN Learn, regarding SSR-related topics such as abuse? It should be noted that ICANN org has in the past provided training and information on DNS abuse and DAAR at ICANN meetings and in various in-person workshops (see example here). ICANN has also published information on credential management to provide contracted parties a background and opportunity to learn practical operational practices for preserving security and stability of the credential management lifecycle. Is the intent of the SSR2 RT's recommendation to go beyond such activities? Is the SSR2 RT recommending that a more formal certification program be created, where, upon completion, parties are "ICANN-certified" in SSR-related issue mitigation?

It is not clear who the intended audience of the training and certification is as the SSR2 RT mentions several parties. Would training and certification be offered to any interested party? Depending on the SSR2 RT's expectations, ICANN org has concerns with the feasibility of implementing such global certification programs. Finally, if the SSR2 RT is referring to more stringent requirements to complete training or certification, such as potential obligations in contracts, this is not within ICANN org's remit to unilaterally impose, as such changes could only come about via consensus policy development or voluntary contract negotiations (as noted by the Board).

SSR2 Recommendation 17.1: ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as inflow, with only summary and metadata flowing upstream. Use of the system should be mandatory for all gTLDs; ccTLDs should be invited to join. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). In addition, reports should be made available (e.g., via email) to non-participating ccTLDs.

ICANN org notes that there are no details or rationale for this recommendation in the "ICANN Compliance" section of the SSR2 draft report. It is difficult for ICANN org to determine how the review team envisions the operational details and measures of success for this recommendation. For this reason, 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.

SSR2 Recommendation 18.1: ICANN org should have compliance activities audited externally and hold them to a high standard.

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. Particularly, ICANN org seeks clarification on the following:

- Who does the SSR2 RT envision conducting the external audit?
- What would the criteria be for an external audit and how would the criteria be applied?
- What is a "high" standard? Who determines that and how is it measured?

Further, ICANN org notes that the RDS-WHOIS2 Review Team reviewed ICANN Contractual Compliance activities (see RDS-WHOIS2 Review Final Report) and made a number of recommendations. The Board took action on the RDS-WHOIS2 recommendations in February 2020 (see RDS-WHOIS2 Recommendations, CC.3 - approved, R4.1 and R4.2 - placed in pending status).

SSR2 Recommendation 18.2: The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes.

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.

SSR2 Recommendation 18.3: The ICANN Compliance Office should, as their default, involve SLAs on enforcement and reporting, clear and efficient processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure.

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?

SSR2 Recommendation 19.2: When misleading naming rises to the level of abusive naming, ICANN org should include this type of abuse in their DAAR reporting and develop policies and mitigation best practices.

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 ongoing discussions related to the definition of “DNS abuse”. However, we are unaware of any consensus within the community on the definition of “misleading”. Beyond this, 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 criteria[1]. ICANN org encourages the SSR2 RT to suggest such a feed for what it considers "misleading" and "abusive" naming to be.

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. See also the ICANN Board comment pertaining to draft recommendations outside of the Board’s oversight responsibilities.

SSR2 Recommendation 20: Complete Development of a DNS Regression Testing

ICANN org is not clear what is meant by “complete development of a DNS regression testing”. ICANN org’s assumption is that there is a typographical error in the draft SSR2 report, leaving out the word “suite” (or something similar), as the text of that recommendation mentions a regression test suite and references the OCTO resolver testbed (which isn’t a regression test suite per se, but could probably be extended).

However, in reading Recommendations 20.1 and 20.2, ICANN org is unsure about the scope of such testing. Regression test suites are never really “complete” as they must always be added to as new issues are identified, and their mitigations deployed. Further, while OCTO has done work in the resolver testbed to test a sampling of open source resolvers, this can in no way be considered complete or even representative of all resolvers that are in use on the Internet today. Finally, the text of 20.3 indicates ICANN org should develop a suite for “DNS regression testing,” but (counter to the “Rationale and Findings" of that recommendation which mentions "resolver behavior") does not limit the functionality to regression test, i.e., it can be read that org should develop a regression test suite for authoritative servers, resolvers, forwarders, etc.

ICANN org asks the SSR2 RT to clarify the intent of this recommendation based on the comments above.

[1] See https://www.icann.org/en/system/files/files/daar-methodology-paper-30nov17-en.pdf for a description on the methodology uses for DAAR and a description of the criteria used to select reputation providers.

SSR2 Recommendation 21: Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers

ICANN org notes that 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.

ICANN org notes that on 15 October 2018, ICANN org determined that the first-ever changing of the cryptographic key that helps protect the DNS was completed with minimal disruption of the global Internet. The communication plan, test pass, and data collection program are all part of the overall KSK Rollover Project, which were established and extensively vetted with the DNS technical community.

SSR2 Recommendation 22.1: ICANN org, in close cooperation with RSSAC and other relevant stakeholders, should ensure that the RSS governance model as proposed by RSSAC037 includes baseline security best practices for root server operators and operations in order to minimize the SSR risks associated with root server operation. These best practices should include change management, verification procedures, and sanity check procedures.

It is ICANN org's understanding that 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.

SSR2 Recommendation 22.2: ICANN org should also develop relevant KPIs to measure the implementation of these best practices and requirements and ensure yearly public reporting on how Root Server Operators (RSOs) and other relevant parties, including ICANN org, can meet these KPIs.

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. It is worth reiterating that ICANN org cannot force the root server operator community to abide by best practices. While it is feasible that ICANN org could ensure yearly public reporting on (publicly published) KPIs, it is unclear what value such reporting would bring. With that said, ICANN org would certainly assist in the development of KPIs and reporting on those KPIs as part of our ongoing support of RSSAC and the GWG if directed by the Board as a result of advice by RSSAC or requested by the GWG.

SSR2 Recommendation 22.3: ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L-Root, and should encourage other RSOs to do the same.

It is unclear what problem this recommendation is trying to solve. Does SSR2 RT believe that IMRS or the other RSOs, either individually or collectively, have insecure infrastructure? Given that documented hardening strategies can provide a “roadmap” to attackers, i.e., identifying weaknesses based on the documented hardening strategy, ICANN org does not feel publishing the strategy we have used to protect IMRS would contribute positively to IMRS security, stability, and resiliency. However, ICANN org does share information with the other RSOs on both operational and security aspects (following FIRST's Traffic Light Protocol).

SSR2 Recommendation 22.4: ICANN org should ensure that the IMRS uses a vulnerability disclosure process (not necessarily public), security reports and intelligence, and communication with researchers and RSSAC advice or recommendations, where applicable.

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.

SSR2 Recommendation 23.2: ICANN org should launch public comment as soon as possible on changes regarding revisions to the RZMS policies.

ICANN org notes that IANA engages with its customers on the development of its technical systems, including Root Zone Management System. Concepts being built into the next generation RZMS are the result of several years of engagement, including discussing concepts with IANA customers and gathering feedback. 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.

SSR2 Recommendation 24.1: ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over.

ICANN org notes that IANA already measures service availability of its critical services as a component of its various SLAs under the IANA contracts. IANA maintains around 3000 registries, mostly served on common architecture that would have the same operational status. 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.

SSR2 Recommendation 25.1: The ICANN community and ICANN org should take steps to ensure that access to CZDS as well as other data is available, in a timely manner, and without unnecessary hurdles to requesters.

ICANN org encourages the SSR2 RT to provide examples of “unnecessary hurdles” that requesters are experiencing. ICANN org notes that ICANN Contractual Compliance provides a complaint form for when users believe registry operators are not complying with the contractual requirements for providing access to zone files. ICANN org also notes, however, that the Registry Agreement does not specify a timeframe in which registry operators must provide zone file access; such a change could only come about through a consensus policy development process or through voluntary contract negotiations (as noted by the Board). Finally, ICANN org notes that the existing CZDS system (which was recently updated and redesigned) provides registry operators an “auto-approve” option for handling requests for zone file access to help expedite approval of access for those registry operators that wish to automate approvals for certain (or all) CZDS users. As noted above, it is helpful for the ICANN org, Board, and community to have an understanding of the particular issues or risks that each recommendation intends to address in order for the Board to properly consider the recommendations and make appropriate instructions to the ICANN org and/or community.

SSR2 Recommendation 25.2: ICANN org should implement the four recommendations in SSAC 97.

ICANN org notes that on 23 June 2018, the Board accepted the advice in SAC097 and directed the ICANN President and CEO or his designee to implement the recommendations contained in SAC097. 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.

SSR2 Recommendation 26.1: ICANN org should publicly document the ERERO processes, including decision points, actions, and exceptions. The document should describe the dependencies for every decision, action, and exception.

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. For example, is the SSR2 requesting the publication of process/procedure documentation, diagrams, flowcharts, FAQs, etc. for how an EBERO event is declared?

SSR2 Recommendation 26.4: ICANN org should improve the process by allowing the gTLD Data Escrow Agent to send the data escrow deposit directly to the EBERO provider

ICANN org requests clarification as to what issues or risks the SSR2 RT intends to address with this recommendation. Further, ICANN org notes that there is no contractual relationship between the EBEROs and the Data Escrow Agents (DEAs) of the gTLDs and while allowing an agent to release escrow file(s) directly to an EBERO provider may remove a process step, it may also add additional complexity (i.e., with maintenance, testing, contracts and costs) because of the need for a new mechanism to release the file(s).

SSR2 Recommendation 27.1: PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security.

ICANN org notes that the Root KSK DNSSEC Practice Statement (DPS) is just one component of implementing operational plans around changing digital signature algorithms, and that such a change must be carefully studied and tested. Such changes do not necessarily create a more resilient DNS if impacts are not properly understood before execution, and many risks pertain to elements — like resolver behavior — that are not under the scope of the DPS. 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.

SSR2 Recommendation 27.2: As root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.

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.

Next steps

ICANN org hopes that the SSR2 RT finds this input useful. We continue our commitment to helping the SSR2 RT complete its important work and may provide additional input as the team's work progresses.

Sincerely,

Göran Marby
ICANN President and Chief Executive Officer