Registries Stakeholder Group Statement

Issue: **Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report**

Date statement submitted: **20 March 2020**

Reference url: https://www.icann.org/public-comments/ssr2-rt-draft-report-2020-01-24-en

Background[1]

The Security, Stability, and Resiliency Review is mandated by ICANN's Bylaws (Article 4, Section 4.6(c)) to review *"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."*

Previous RySG comments on the issue:

- RySG Comment Final Report SSR1 (July 2012) https://forum.icann.org/lists/ssr-rt-final-report/docx509KspLXv.doc
- RySG Comment Draft Report SSR1 (April 2012) https://forum.icann.org/lists/ssrt-draft-report/doc3FGcXvtjyX.doc

---

Registries Stakeholder Group comment:

Introduction & Overarching comments

Note: We observe that the numbering of the points within each recommendation in the body of the report does not match the numbering in the table on pages 7-21 (e.g., the table notes Recommendation 2 has points 2.1-2.5 but the body at page 23 starts Recommendation 2 at 2.6). We refer throughout to the numbering in the table, for ease.

The Registries Stakeholder Group (RySG) thanks the SSR2 Review Team for its diligent work. The format of the report is easy to follow and clearly set out, and we appreciate the inclusion of SSR2's rationale for each conclusion. However, we do believe that **the proposed recommendations would benefit from an explicit statement of the problem that each over-arching recommendation is intended to address.**

[1] *Background: intended to give a brief context for the comment and to highlight what is most relevant for RO's in the subject document – it is not a summary of the subject document.*

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. Amendments to the registry agreement are only possible via a formal amendment process or the adoption of consensus policies. **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.**

At a time when ICANN and the community are struggling to prioritise and respond to various work efforts, we are concerned by the broad scope and the actual number of recommendations contained within the Draft Report. Simply put, we do not believe ICANN and the community have the bandwidth for 26 high-priority recommendations, many with multiple subsections, (plus all of the unfinished SSR1 work, which is also a high priority). Labeling 26 out of 31 recommendations as high priority is not helpful and statements such as 'All SSR2 RT recommendations align with ICANN org's strategic plan, and so are considered high priority' (p. 7) give the wrong signal. **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.**

Further, various recommendations (including 11, 14, 15 and 16) amount to restatements of recommendations made by the CCT-RT in its Final Report of October 2018. Many of those recommendations were put into a "pending" category by the ICANN Board and it is worth noting that many of them were met with significant objection by the Contracted Parties, among other community members. Again, we fail to understand what the SSR2-RT was hoping to accomplish by resubmitting nearly identical recommendations to the same ICANN Board that is still struggling to respond to the original ones. The RySG appreciates that the SSR2 has done its work thoroughly, but is concerned about the time and resources spent on re-doing work already completed by another review team. **We would appreciate additional information from the SSR2-RT about how it reached the decision to effectively duplicate the recommendations from a previous Review Team.**

Prior to the publication of the SSR2-RT Final Report, the RySG encourages **the SSR2-RT to spend some additional time considering what it hopes to achieve by reiterating CCT-RT recommendations, and reconsider whether they are truly necessary within an otherwise very robust set of recommendations. The RySG considers the implementation and completion of outstanding SSR1 recommendations as the key priority.** In particular, the RySG believes that the remit of SSR needs to be clearly defined so that it can properly inform the scope of SSR2's work and can provide the Board with some guidance on the new recommendations. The RySG generally supports the SSR1 recommendations and flags our concerns below.

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.** The RySG appreciates that it is useful for the SSR2 to have a working glossary to assist its work, but the working glossary should not be used to interpret the recommendations made by SSR2, or adopted as community definitions by the Board. The report seems to repeatedly conflate the terms to broadly encompass

undesirable activity related to both DNS/infrastructure abuse, security threats, and IP/content-related abuse.

Finally, and critically, **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.** Reviews, while an important part of ICANN's accountability mechanisms, cannot be used to circumvent the policy development process, such as by attempting to impose new contractual obligations on contracted parties. The RySG would also ask SSR2 to refrain from making recommendations which refer to, or overlap with, existing recommendations from other reviews such as RDS-WHOIS 2, CCT-RT, Registration Data EPDP Phase 2, NCAP and potential recommendations from ATRT3.

Comments on the individual recommendations

Recommendation #1 (priority High) **Complete the implementation of all relevant SSR1 recommendations**

RySG comment:

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

Recommendation #2 (priority High) **SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications** 2.1. ICANN org should establish a road map of its industry-standard security audits and certification activities that are being undertaken, including milestone dates for obtaining each certification and noting areas of continuous improvement. 2.2. ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies. 2.3. ICANN org should also provide reasoning for their choices, demonstrating how they fit into its security and risk management strategies 2.4. ICANN org should implement an Information Security Management System and undergo a third-party audit. 2.5. In order to reap the benefits of a certification and audit regimen, ICANN org should be audited and certified by a third party along the lines of industry security standards and should assess certification

options with commonly accepted international standards (e.g., ITIL, ISO 27001, SSAE-18) for its operational responsibilities.

RySG comment:

The RySG supports this recommendation.

Whilst it is encouraging to see progress made regarding ICANN org's pursuit of various certifications, conducting internal audits and providing security training, it remains unclear how these are structured into a clear roadmap and overarching strategy. The RySG shares the concerns raised by the SSR2 team that ICANN org's approach appears to be ad hoc and the indications that industry best practices are not followed (e.g. by not rotating auditors regularly).

Recommendation #3 (priority High)

SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures

3.1. ICANN org should address security issues clearly, publicly (with consideration for operational security, e.g., after an established moratorium and anonymization of the information, if required), and promote security best practices across all contracted parties.

3.2. ICANN org should also capture SSR-related best practices in a consensus document, establish clear, measurable, and trackable objectives, and then implement the practices in contracts, agreements, and MOUs.

3.3. ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues should be communicated promptly to trusted, relevant parties (e.g., those affected or required to fix the given issue), such as in cases of breaches at any contracted party and in cases of key vulnerabilities discovered and reported to ICANN org.

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.

RySG comment:

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.

Recommendation #4 (priority Medium)

SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs

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.

RySG comment:

The RySG supports this recommendation.

Recommendation #5 (priority High)

SSR1 Recommendation 27 - Risk Management

5.1. ICANN's Risk Management Framework should be centralized and strategically coordinated.

5.2. ICANN org should clearly articulate their risk framework and strategically align the framework against the requirements and objectives of the organization, describing relevant measures of success and how ICANN org will assess these measures.

5.3. ICANN should make information pertaining to risk management centrally available to the community. This information should be regularly updated to reflect the current threat landscape (at least annually).

RySG comment:

The RySG supports this recommendation and suggests that it is bundled with recommendations 7, 8 and 9.

Recommendation #6 (priority High)

Create a Position Responsible for Both Strategic and Tactical Security and Risk Management

6.1. ICANN org should create a position responsible for both strategic and tactical security and risk management across the internal security domain of the organization, as well as the external global identifier system.

6.2. ICANN org should hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions.

6.3. This position should manage ICANN org's Security Function and oversee the interactions of staff in all relevant areas that impact security.

6.4. The position should also provide regular reports to ICANN's Board and community.

6.5. This position would act as a pathfinder and problem-solver who would strategize and execute multi-faceted programs to achieve substantial improvements.

6.6. Additionally, this role should take part in all security-relevant contractual negotiations (e.g., supply chains for hardware and software and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.

RySG comment:

The RySG does not support this recommendation.

We agree that ICANN may not currently have one single-threaded owner for SSR-related work and budgets (though we agree OCTO is performing some of these functions and the Board or Finance are performing others), but we believe this can be accomplished with the resources available. Given there is a distinction between the management of internal ICANN IT systems that seems to be under the purview of ICANN's Chief Information Officer and ICANN's responsibility for the security and stability of the DNS that is the remit of the Chief Technology Officer, perhaps it would be more realistic to recommend more transparency of areas of duplication and clarity as to lines of responsibility.

Recommendation #7 (priority High)

Further Develop a Security Risk Management Framework

7.1. ICANN org should clearly articulate their Security Risk Management Framework and ensure that it aligns strategically against the requirements and objectives of the organization.

7.2. ICANN org should describe relevant measures of success and how these measures are to be assessed. The SSR2 RT described the foundation of this in detail in the additional feedback regarding SSR1's Recommendation 9 (see 'SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications' earlier in this report).

7.3. ICANN org should:

7.3.1. Adopt and implement ISO 31000 "Risk Management" and validate and certify their implementation with appropriate independent audits.[4] Risk management efforts should feed into Business Continuity and Disaster Recovery Plans and Provisions.

7.3.2. Regularly update a register of security risks and use that register to prioritize and guide the activities of the ICANN org. ICANN org should report on updates of their methodology and updates to the register of security risks. Findings should feed into BC/DR and the Information Security Management System (ISMS).

7.3.3. Name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role as described in the recommendation "C-Suite Security Position."

RySG comment:

The RySG supports this recommendation and suggests that it is bundled with recommendations 5, 8 and 9.

Recommendation #8 (priority High)

Establish a Business Continuity Plan Based on ISO 22301

8.1. ICANN org should establish a Business Continuity Plan for all the systems owned by, or under the purview of ICANN org,based on ISO 22301 "Business Continuity Management."[5]

8.2. ICANN should identify the importance of functional, acceptable timelines for BC and DR based on the urgency of restoring full functionality.

8.3. For Public Technical Identifiers (PTI) operations (IANA functions, including all relevant systems that contribute to the Security and Stability of the DNS and also Root Zone Management), ICANN org should develop a shared approach to service continuity in close cooperation with the Root Server System Advisory Committee (RSSAC) and the root server operators.

8.4. ICANN org should publish evidence (e.g., a summary) of their Business Continuity Plans and Provisions. An external auditor should be engaged to verify compliance aspects of the implementation of the resulting business continuity plans.

RySG comment:

The RySG supports this recommendation and suggests that it is bundled with recommendations 5, 7 and 9.

Recommendation #9 (priority High)

Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented

9.1. ICANN org should ensure that the DR plan for PTI operations (IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031 *Guidelines for information and communication technology readiness for business continuity.* ICANN org should develop this plan in close cooperation with RSSAC and the root server operators.

9.2. ICANN org should also establish a DR Plan for all the systems owned by or under the purview of ICANN org, again in line with ISO 27031 *Guidelines for information and communication technology readiness for business continuity.*

9.3. ICANN org should have a disaster recovery plan developed within twelve months of the ICANN Board's adoption of these recommendations around establishing at least a third site for disaster recovery (in addition to Los Angeles and Culpepper), specifically outside of the United States and its territories and the North American region, including a plan for implementation.

9.4. ICANN org should publish a summary of their overall disaster recovery plans and provisions. ICANN org should engage an external auditor engaged to verify compliance aspects of the implementation of these DR plans.

RySG comment:

The RySG supports this recommendation and suggests that it is bundled with recommendations 5, 7 and 8.

Recommendation #10 (priority High)

Improve the Framework to Define and Measure Registrar & Registry Compliance

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.[6,7]

10.2. Allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics.

10.3. Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident).

10.4. Further, the ICANN Board should take responsibility for bringing the EPDP[8] to closure and passing and implementing a WHOIS policy in the year after this report is published.

RySG comment:

The RySG notes that Compliance's size and scope has grown exponentially in recent years and 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. We note this throughout the report, but call it out specifically here.

10.1 – Compliance-related recommendations must be linked to specific contract terms. "Other elements that affect abuse, security, and resilience" is too vague to be implementable. The RySG believes this is out of scope of SSR2.

10.2 – The RySG does not see the value in specific compliance officers to handle specific contractual compliance issues. All of Compliance is capable of responding to compliance complaints and ICANN has demonstrated that it's capable of conducting a full audit of all Ry contracts on a specific issue, like SLAs.

10.3 – The RySG believes that this is outside the scope of the SSR2's work. The RySG notes that there is an established contract amendment process: consensus policy and negotiations between CPs and ICANN. This recommendation has no basis in policy or fact - it is a conclusory statement that presupposes the question. If the SSR2 has identified problems with performance metrics, then it could recommend that ICANN and the community study them. In this case, the SSR2 is proceeding down the same slippery slope as CCT-RT in recommending solutions without recommending ICANN first engage in exploration and work to determine if a solution is needed.

10.4 – 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).

Recommendation #11 (priority High)

Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions

11.1. ICANN Board should drive efforts that minimize ambiguous language and reach a universally acceptable agreement on abuse, SSR, and security threats in its contracts with contracted parties

and implementation plans.

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[9].

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[10] and for Specification 11[11]), and addressed in international conventions such as the Convention on Cybercrime and its related "Explanatory Notes" [12] —to use in conjunction with ICANN org's DNS Abuse definition.[13]

11.4. The ICANN Board should entrust SSAC and PSWG to work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime.

RySG comment:

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.

11.2 – The RySG is unclear about what the SSR2 is asking given Recommendation 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.

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 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".

11.4 – The RySG believes this is a policy matter and outside the scope of SSR reviews - if the Board would like the community to try to define DNS abuse, then it can instruct the community to do so, but it's inappropriate to recommend that the definition come solely from two ACs (SSAC and GAC) without input from the rest of the community.

Recommendation #12 (priority High)

Create Legal and Appropriate Access Mechanisms to WHOIS Data

12.1. The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement.

12.2. The ICANN Board should take responsibility for, and ensure ICANN org comes to immediate closure on, implementation of the Temporary Specification for gTLD Registration Data.

RySG comment:

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.

Recommendation #13 (priority High)

Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program

13.1. The ICANN Board and ICANN org should work with the entities inside and outside the ICANN community that are mitigating abuse to improve the completeness and utility of DAAR, in order to improve both measurement and reporting of domain abuse.

13.1.1. ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology.

13.1.2. ICANN org should make the source data for DAAR available through the ICANN Open Data Initiative and prioritize items *"daar"* and "*daar-summarized*" of the ODI Data Asset Inventory[14] for immediate community access.

13.1.3. ICANN org should publish reports that include machine- readable formats of the data, in addition to the graphical data in current reports.

13.1.4. ICANN org should provide assistance to the Board and all constituencies, stakeholder groups and advisory committees in DAAR Interpretation, including assistance in the identification of policy and advisory activities that would enhance domain name abuse prevention and mitigation.

RySG comment:

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.

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.

13.1.2 and 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.

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.

Recommendation #14 (priority High)

Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse

14.1. ICANN org should collect, 11nalyse, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse.

RySG comment:

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

The RySG notes that ICANN is not a price regulator and is unclear what benefit would come from this research. Further, the RySG is concerned that this recommendation presupposes a relationship between the price of domain names and evidence of "security threats and abuse". The RySG refers to its previous comments on collecting pricing data made in response to the CCT-RT Final Report, particularly recommendations 2, 3, and 4. (link)

Recommendation #15 (priority High)

Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse

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.[15]

15.2. ICANN org should introduce a contract clause that would support contract termination in the case of "a pattern and practice" of abuse (as in section 5.5.2.4 "TERM, TERMINATION AND DISPUTE RESOLUTION" of the 2013 Registrar Accreditation Agreement)[16].

15.3. In order to support the review of these contract changes, ICANN org should:

15.3.1. Ensure access to registration data for parties with legitimate purposes via contractual obligations and with rigorous compliance mechanisms.

15.3.2. Establish and enforce uniform Centralized Zone Data Service requirements to ensure continuous access for SSR research purposes.

15.3.3. Attract and collaborate with ccTLDs and the ccNSO to help address DNS abuse and security threats in ccTLDs.

15.3.4. The ICANN Board, community, and org should work with the ccNSO to advance data tracking and reporting, assess DNS abuse and security threats in ccTLDs, and develop a ccNSO plan to support ccTLDs in further mitigating DNS abuse and security threats.

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.

15.4. In the longer term, ICANN Board should request that the GNSO initiate the process to adopt new policies and agreements with Contracted Parties that measurably improve mitigation of DNS abuse and security threats, including changes to RDAP and registrant information, incentives for contracted parties for abuse/security threat mitigation, establishment of a performance metrics framework, and institutionalize training and certifications for contracted parties and key stakeholders.

RySG comment:

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. Similarly, the ICANN Board has no authority to implement the recommendation/s.

The RySG opposes this recommendation because it presupposes the outcome of work that should be done by the community and, in several places, seems to try to preempt (and end-run around) work being done in the community and by other PDPs, such as the EPDP. Furthermore this recommendation is wholly outside the scope of the SSR2's remit (e.g. setting threshold to trigger "automatic" contract defaults). Perhaps the scope of SSR3 will be to review the outcome of the various work in progress today, but this RT is not tasked with using the Recommendations of the RT to hammer home viewpoints on how the Board and the community should presume to resolve ongoing work.

Recommendation #16 (priority High)

Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats

16.1. ICANN org should incentivize the mitigation of abuse and security threats making the following changes to contracts:

16.1.1. 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).

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

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.

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).

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.

RySG comment:

Again, the RySG opposes this recommendation because it's outside the scope of the RT's role.

Incentives, both negative and positive, concerning mitigation of domain abuse are potentially problematic depending on evolving definitions of abuse, especially "abusive naming", different market positions of TLDs, and the potential for manipulation of results. For example, particularly desirable TLDs may be more prone to some types of "abuse," through no fault of the registry.

Publishing and creating incentives around abuse statistics invites manipulation by competitors or could result in undesirable and unforeseen abusive pattern shifts. For example, registering significant numbers of "abusive" domains in order to damage competitor statistics could trigger problematic contract clauses or increasing prices.

The recommendations of enhancing contracts with registrars and registries to incent the mitigation of DNS abuse (including the right for ICANN to invoke presumptive contract default) are established on a lack of data that showcases what the implication of altering the economic underpinning of a highly competitive market would entail, including inadvertent side effects such as registries that already sell low price domains being rewarded with lower ICANN fees. The recommendations in this section need to be developed by the community, not in Review Teams. The RT's recommendations should focus on gaps in ICANN's handling of security, stability, and resilience.

Recommendation #17 (priority High)

Establish a Central Abuse Report Portal

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.

RySG comment:

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.

Recommendation #18 (priority High)

Ensure that the ICANN Compliance Activities are Neutral and Effective

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

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.

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.

RySG comment:

The RySG is unclear why this recommendation is being made.

Although SSR2 flags that the contractual obligations are implemented differently by each contracted party, the RySG notes that the contracts do not prescribe uniform or required mechanisms for contracted parties to meet their obligations. There is presently no SLA that can be pointed to in order to determine, unequivocally, that a contracted party is "aiding and abetting systemic abuse," nor does it make sense to try to measure contracted party behavior in this way.

This recommendation should be reconsidered.

Recommendation #19 (priority High)

Update Handling of Abusive Naming

19.1. ICANN org should build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable.

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.

19.3. ICANN org should publish the number of abusive naming complaints made at the portal in a form that allows independent third parties to analyze, mitigate, and prevent harm from the use of such domain names.

19.4. ICANN org should update the current "Guidelines for the Implementation of IDNs" **[citation to be added]** to include a section on names containing trademarks, TLD-chaining, and the use of (hard-to-spot) typos. Furthermore, ICANN should contractually enforce "Guidelines for the Implementation of IDNs" for gTLDS and recommend that ccTLDs do the same.

RySG comment:

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

If the SSR2 believes there are specific security concerns related to naming use cases, then it should make recommendations for the community to study them. For instance, the concepts of "misleading naming" (e.g. visually indistinguishable, "hard to spot" typos) and "abusive naming" need to be better and more precisely defined to avoid subjective interpretations. The precision means not only a precise definition or list, but also that any phrase along the lines of "including but not limited to" must be avoided. "Abusive naming" should be constrained to security threats to DNS and not include web content (which is squarely outside ICANN's remit). Web content abuses have their own set of issues and solutions, such as TMCH, UDRP and URS.

Further, it is important that policies around DNS Abuse strike a balance between meeting the need of users wanting an online identifier and addressing security concerns. RySG advises the RT to acknowledge the distinction between malicious registration and compromised domain name. While

we note some domain names could be registered in bad faith, not all "abusive naming" originated as is but domain names were compromised at some point in time, by malware or other means. Which is why registries are supportive of an approach that leans towards monitoring as opposed to blocking a registration.

The RT bases its conception of "misleading naming" on the idea of what content a user "expects" to find based on the name, which is entirely unknowable by the parties expected to enforce against it. Case in point, the RT asserts that a name containing a trademark should be considered misleading naming. Given that any word could be a trademark, that each country has its own trademark database(s), and that eligibility and standards regarding trademarks vary widely from country to country, taking action against "misleading naming" based on trademark inclusion becomes impossible.

19.4 – The ICANN IDN Guidelines should not duplicate, potentially putting itself in conflict with the Registry Agreement or ICANN policies, what otherwise can be applied in a more general way to all types of domain names, ASCII and IDN.

For example, Specification 7 (Rights Protection Mechanisms) of the 2017 Base Registry Agreement applies equally to all domain name registration regardless of the script used.

Further, there seems to be the incorrect perception that ICANN does not enforce the IDN Implementation Guidelines upon gTLD registries, when the opposite is true. ICANN uses the Registry System Testing process to evaluate registry operator's implementation of the IETF Standards and IDN Guidelines (i.e. Specification 6 of the 2017 Base Registry Agreement), prior to delegation and when required by a new Registry Service Evaluation Process. If the registry operator does not meet the requirement as set forth in their registry agreement, then the registry operator needs to remediate the issues before ICANN approves any registry service.

Recommendation #25 (priority High)

Ensure the Centralized Zone File Data Access is Consistently Available

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.

25.2. ICANN org should implement the four recommendations in SSAC 97:[19]

"Recommendation 1: The SSAC recommends that the ICANN Board suggest to ICANN Staff to consider revising the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default. This could include an option allowing a registry operator to depart from the default on a per- subscriber basis, thereby forcing the chosen subscriber to reapply at the end of the current term. The CZDS should continue to provide registry operators the ability to explicitly terminate a problematic subscriber's access at any time.

Recommendation 2: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that in subsequent rounds of new gTLDs, the CZDS subscription agreement conform to the changes executed as a result of implementing Recommendation 1.

Recommendation 3: The SSAC recommends that the ICANN Board suggest to ICANN Staff to seek ways to reduce the number of zone file access complaints, and seek ways to resolve complaints in a timely fashion.

Recommendation 4: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that zone

file access and Web-based WHOIS query statistics are accurately and publicly reported, according to well-defined standards that can be uniformly complied with by all gTLD registry operators. The Zone File Access (ZFA) metric should be clarified as soon as practicable.

RySG comment:

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.

25.2 – The RySG notes that the four recommendations flagged by the SSR2 have already been accepted by the ICANN Board according to this Board resolution https://www.icann.org/resources/board-material/resolutions-2018-06-23-en#1.g. 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.

Recommendation #28 (priority Medium)

Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution

28.1. ICANN org should produce findings that characterize the nature and frequency of name collisions and resulting concerns. The ICANN community should implement a solution before the next round of gTLDs.

28.2. ICANN org should facilitate this process by initiating an independent study of name collisions through to its eventual completion and adopt or account for the implementation or non-adoption of any resulting recommendations. By"independent," SSR2 RT means that ICANN org should ensure that the SSAC Name Collision Analysis Project (NCAP) work party research and report evaluation team's results need to be vetted by parties that are free of any financial interest in TLD expansion.

28.3. ICANN org should enable community reporting on instances of name collision. These reports should allow appropriate handling of sensitive data and security threats and should be rolled into community reporting metrics.

RySG comment:

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.

Recommendation #29 (priority High)

Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements

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).

29.2. ICANN org's consensus policies and agreements with registry operators and registrars should,

therefore, have clauses to reflect compliance with these while ensuring that the DNS is not fragmented because of the need to maintain/implement minimum requirements governing the collection, retention, escrow, transfer, and display of registration data, which includes contact information of the registrant, administrative, and technical contacts as well as technical information associated with a domain name.

29.3. ICANN org should:

29.3.1. Create specialized units within the contract compliance function
that focus on privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the evolving RDAP framework.

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.[20]

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.

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.

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.

RySG comment:

While the RySG supports ICANN tracking new technology and evolving privacy laws and regulations as part of its overall risk management management, the RySG believes that much of this recommendation is out of scope for SSR2. Specifically, we oppose the creation of specialized compliance officers to micromanage contracted party operations. Registries and registrars are responsible for complying with all local laws - ICANN's compliance team doesn't need to duplicate the function of local law enforcement. The RySG also notes its support for recommendation 31.

Recommendation #30 (priority Medium)

Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates

30.1. ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE S&P, as well as the operational security conferences APWG, M3AAWG, and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior.

30.1.1. These reports should include recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature.

30.1.2. These reports should also include recommendations for additional study to confirm peer-reviewed findings, a description of what data would be required to execute additional recommended studies, and how ICANN can offer to help broker access to such data, e.g., CZDS.

RySG comment:

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

Recommendation #31 (priority High)

Clarify the SSR Implications of DNS-over-HTTP

31.1. ICANN org should commission an independent investigation(s) into the SSR-related implications of DoH deployment trends, as well as implications for the future role of IANA in the Internet ecosystem. The intended outcome is to ensure that all stakeholders have the opportunity to understand the SSR- related implications of these developments, and the range of alternatives (or lack thereof) various stakeholders have to influence the future.

RySG comment:

The RySG supports this recommendation.