Public Interest Registry Comments to the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report Public Comment Period
10 March 2021

Public Interest Registry appreciates the opportunity to provide comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report (the Report). We fully support the comments submitted by the Registries Stakeholder Group and take this opportunity to further highlight certain critical issues and concerns with the SSR2 Final Report.

PIR is concerned that several of the SSR2 Final Report recommendations venture outside SSR2 Review Team's remit by recommending actions that would violate the terms of the Base gTLD Registry Agreement (Registry Agreement) and attempt to circumvent the multistakeholder policy development process.

Overarching Concerns

Several recommendations in the Report recommend that ICANN attempt to make unilateral changes to the Registry Agreements. Changes to Registry Agreements of this sort should only be made via the GNSO Policy Development Process resulting in a Consensus Policy or via triggering a formal negotiation process under the terms of the Registry Agreement. Further, several SSR2 recommendations would represent violations of the terms of the Registry Agreement which governs the inclusion of third-party interests in contractual negotiations and how temporary policies/specifications may be used by ICANN. Other recommendations imply that ICANN Compliance is not enforcing existing contractual obligations or encourage ICANN Compliance to undertake activities that are clearly outside of ICANN Compliance's scope and remit. Finally, we note that several recommendations represent significant duplication of ongoing cross community work and recommendations from the CCT RT, many of which focus on the issue of DNS Abuse.

Supporting Continued Cross Community Cooperation on DNS Abuse

PIR takes the issue of DNS Abuse very seriously and has established itself as an industry leader in efforts to combat DNS Abuse. To maintain our commitment to our registrants and maintain .ORG as the most trusted domain space, we've undertaken both internal efforts to ensure our anti-abuse policies are robust and fair, and external work across the ICANN community and industry to develop real solutions and tools to combat DNS Abuse.

PIR worked with fellow industry leaders to develop the Framework to Address Abuse, where signatories clearly state when they believe registries and registrars must act on DNS Abuse. In addition, the Framework outlines where, regardless of contractual obligations, registries and registrars should act. The Framework was developed and launched in October 2019 with 11 signatories and grew in a little over a year to include 50 of the largest registries and registrars in the industry. The Framework, along with the Internet and Jurisdiction Policy Network's Operational Approaches, Norms, Criteria, Mechanisms, served as a basis for the development and adoption of a Contracted Parties House definition of DNS Abuse, which is a realistic framework to refine and target cross community engagement to combat DNS Abuse.

In addition to developing the Framework to establish guidance for industry policy and practice, PIR has implemented the Quality Performance Index (QPI) as a proactive measure to reduce DNS Abuse and to incentivize registrars to lower their own abuse rates. QPI uses a quality score to encourage "healthy" (e.g., responsible and non-abusive) domain name registrations and accurately measure the quality of individual registrar's .ORG domain names. QPI has been well received by registrars and the community and was featured as a Registry Best Practice by ICANN's Government Advisory Committee's Public Safety Working Group. QPI has been so well received that in March 2021, PIR announced that it will be making QPI freely available to registries interested in deploying the tool to improve the quality of their

own spaces. From our own experience we believe that expansion of QPI will benefit the domain space and Internet as a whole by enabling registries to identify best practices and incentivize registrars to reduce abuse rates and increase TLD usage and renewals.

PIR has also updated our processes to ensure our policies respect, and our registrants enjoy, rights such as freedom of expression, due process, and transparency when PIR weighs decisions around abuse. PIR has developed and implemented Anti-Abuse Principles to guide our efforts and set standards for how PIR operates with regard to abuse. PIR operationalized the core principle of due process by creating an Anti-Abuse Policy Appeals Mechanism which provides an opportunity to dispute decisions to suspend domain names under our Anti-Abuse Policy.

Finally, because PIR believes so strongly in supporting dialogue and developing resources for the industry, in February 2021 we launched the DNS Abuse Institute. The DNS Abuse Institute will focus on: innovation by creating recommended practices, research, and practical solutions to combat DNS Abuse; collaboration by serving as a networking forum and central sharing point for interested stakeholders; and education as a resource for stakeholders to access a library of information and practices, abuse mitigation standards, and research on DNS Abuse.

These efforts, and the support and adoption by the industry at large, demonstrate the ability for a community of varied stakeholders including government, law enforcement, and industry to collaborate on complicated issues and to craft real solutions.

Specific Contractual Concerns

PIR does not support recommendations that suggest unilateral contractual changes by the ICANN Board as this action is not supported by a procedural or contractual mechanism. PIR understands and appreciates the SSR2 Review Team's goal to provide measurable actions to address security and stability issues and, as stated in their recent webinar, their desire to create "SMART" recommendations. However, Review Team recommendations cannot ignore the policy development process or recommend implementation that would violate contractual terms merely in the name of consistency.

Specifically, Recommendations 8 and 14 are not consistent with the terms of the Registry Agreement. Recommendation 8 violates several provisions of the Registry Agreement. Section 7.7 of the Registry Agreement allows for the bilateral negotiation of a contemplated change to the Registry Agreement between Registries and ICANN itself, but not third parties that are not a party to the Agreement. The Registry Agreement does provide for the possibility of a "Working Group" participating in these negotiations. Only Registries make such an appointment.[1] Further, the Registry Agreement explicitly states that there are no third-party beneficiaries to the Registry Agreement.[2]

Recommendation 14 violates the terms of the Registry Agreement that govern how temporary policies/specifications may be utilized by ICANN.[3] In addition, the terms Stability and Security are not amorphous or generic concepts in the Registry Agreement, but rather are defined terms.[4]

---

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

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

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

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

A temporary policy/specification is a contractual tool set forth in the Registry Agreement and is not intended to usurp or circumvent ongoing Community discussion or of the multistakeholder policy development process itself. Recommendation 14 fails to meet the requirements for temporary specifications contained in the Registry Agreement in several key ways: (1) a temporary specification must be as "narrowly tailored" as feasible to achieve its defined purposes; and (2) Temporary Specifications must address an immediate need to preserve the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues.[5]

In addition, under the Registry Agreement the ICANN Board must articulate an immediate need to protect the "Stability or Security of the DNS" and narrowly tailor the temporary specification to achieve that goal. The requirement that any temporary specification be "narrowly tailored" to achieve its stated objectives is an intentional and overtly high bar because temporary specifications, if abused, would undermine Community discussions and the multistakeholder process itself.[6]

One of the primary restrictions on temporary specifications is that the measures contained therein must be immediately required to preserve the Security and Stability of the DNS. Recommendation 14 fails to meet that requirement in a number of ways. The Review Team has not articulated a new threat to the Security or Stability of the DNS, rather, they describe active policy discussions around DNS Abuse within the ICANN Community.

Multistakeholder Policy Development Process

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

An EPDP may only be initiated in the limited circumstances to "(1) to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the Board or the implementation of such an adopted recommendation; or (2) to create new or additional recommendations for a specific policy issue that had been substantially scoped previously such that extensive, pertinent background information already exists, e.g. (a) in an Issue Report for a possible PDP that was not initiated; (b) as part of a previous PDP that was not completed; or (c) through other projects such as a GGP."[7] Further, it's the GNSO, not the Board, that determines if these limited conditions have been met and if an EPDP should be initiated. The recommendation also attempts to predetermine the

---

… [A]n effect on "Stability" shall refer to (1) lack of compliance with applicable relevant standards that are authoritative and published by a well-established and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice Requests for Comments ("RFCs") sponsored by the Internet Engineering Task Force; or (2) the creation of a condition that adversely affects the throughput, response time, consistency or coherence of responses to Internet servers or end systems operating in accordance with applicable relevant standards that are authoritative and published by a well-established and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice RFCs, and relying on Registry Operator's delegated information or provisioning of services."

[5] The legal standard for "narrowly tailored" is an incredibly restrictive one. Under US law (which governs the terms of the Registry Agreement) the "narrowly tailored" legal standard is associated with the "strict scrutiny" test to evaluate laws relating to restrictions on the content of speech or laws challenged for racial discrimination grounds. This standard is one of the most rigorous standards in the legal system.# In cases utilizing the strict scrutiny/narrowly tailored tests, the government must have articulated a "compelling governmental interest" and must have "narrowly tailored" the law to achieve that interest; Base TLD Registry Agreement Spec. 1, §2.1, https://www.icann.org/sites/default/files/tlds/org/org-agmt-pdf-30jun19-en.pdf

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

[7] Annex A-1: GNSO Expedited Policy Development Process. https://www.icann.org/resources/pages/governance/bylaws-en/#annexA1

participation, scope, and outcomes of an EPDP which disregards the role of the GNSO and the multistakeholder policy development process.

As with Recommendation 14, we reiterate that the issue of DNS Abuse is not narrowly defined by the Report and is already the subject of ongoing cross community work that has shown real outputs.

PIR is supportive of continued engagement across the ICANN community as the most effective vehicle to address issues related to combatting DNS Abuse. Cross community engagement has already resulted in an increase in accepted best practices and a downward trend of DNS Abuse, as noted by ICANN's Office of the CTO, and we believe there continues to be opportunity for improvement in how the industry addresses DNS Abuse.[8]

[8] ICANN, "*Abuse Across the DNS" since ICANN66 (and before),* November 2020, available at https://cdn.filestackcontent.com/content=t:attachment,f:%22DNS%20Abuse%20Plenary%20Session.pdf%22/ZUoSPQHkRHOOwTWEsTA1; *About Spam*, The only category of abuse that went up was spam, which as ICANN has previously, noted is outside of its remit. ICANN, available at https://www.icann.org/resources/pages/spam-2013-05-03-en; Registries Stakeholder Group Comment to the SSR2 Final Report, Registries continue to work across the community to combatDNS Abuse, including working with the Public Safety Working Group in creating the Framework for Registry Operators to Respond to Security Threats, which provides helpful guidance for registries in addressing DNS Abuse. As well as their work with ICANN Org to publish the Specification 11(3)(b) Advisory, that explains registry obligations regarding identifying DNS Abuse in a gTLD's registrations.