Registries Stakeholder Group Statement

Public Comment: **Second Security, Stability, and Resiliency (SSR2) Review Team Final Report**

Date statement submitted: **9 March 2021**

Reference url: *https://www.icann.org/public-comments/ssr2-final-report-2021-01-28-en* .

Background[1]

The **SSR2 Review Team Final Report** (.pdf) is issued for Public Comment to inform Board action on the SSR2 Review Team's final recommendations. Per the ICANN Bylaws (Section 4.6(a)(vii)(C)), the Board shall consider the SSR2 Review Team Final Report within six months of receipt of the final report, i.e. by 25 July 2021.

The **RySG commented on the SSR2 Review Team's Draft Report** on 20 March 2020.

Registries Stakeholder Group comment

The Registries Stakeholder Group (RySG) welcomes the opportunity to comment on the second Security, Stability, and Resiliency (SSR2) Review Team Final Report and appreciates the amount of time and effort dedicated to the work of the SSR2 Review Team Report.

Overarching comments

Some of the recommendations made by the Review Team advocate for changes to foundational elements of the multistakeholder model, which we find concerning. Specifically:

- As the RySG noted in response to the SSR2 Draft Report, several recommendations suggest direct changes to the Registry Agreement. **Changes to Registry Agreements may only be made through the policy development process or by triggering a formal negotiation and amendment process.** While the RySG appreciates the goal of the SSR2 to highlight issues of concern, we are concerned that this input was not adopted by the SSR2 in its Final Report. Several recommendations in the Final Report continue to rely upon unilateral action at the Board level.

- The Report includes recommendations directing the Board to mandate the inclusion of third party interests in contractual negotiations. The RySG encourages community-wide

[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.*

discussion and cooperation on issues of concern. This unilateral direction is outside the scope of the Board's power. In addition, implementation of recommendations to include or represent third party interests in contractual negotiations would violate existing terms in the Registry Agreement. **The RySG urges the ICANN Board to reject recommendations where the implementation would represent a violation of contractual provisions or ICANN policy development processes.**

- As the RySG noted in its comments to the SSR2 Draft Report, **we cannot support recommendations that repeat, or represent significant overlap with, recommendations of other active reviews such as the CCT-RT and policy processes such as the EPDP.** The RySG questions the value in implementing repetitive recommendations and urges the Board to consider the impact on the workloads of the community and Staff, and to reject those where implementation would circumvent the policy development process or where similar past recommendations have not been accepted by the Board.

- In an effort to create SMART recommendations the Report focuses on tactics and actions and does not include **adequate problem statements to support the recommended actions**.

- DNS Abuse is a topic of discussion across the community, and considerable attention is given to the topic by the Report. Any community-wide debate benefits from clarity in terminology and definitions. However, we note that the Review Team's Report lacks an explicit reference of the definition applied to their consideration of DNS Abuse. Further, we would like to **urge the Board to consider the wealth of DNS Abuse work that is ongoing in the community and to not accept recommendations that would duplicate those efforts or risk to undo progress made in recent months.**

  For example, the RySG recently successfully completed the work of its DAAR Working Group, whose purpose was to engage with OCTO and evolve elements of DAAR to be more informative to the community. It was a successful partnership that continues today with the RySG's DNS Abuse Working Group. The RySG DNS Abuse Working Group has a broader charter to consider all issues related to DNS Abuse with the ICANN community as they relate to registries. It is working in partnership with the RrSG's DNS Abuse Working Group. Our joint agenda is currently focused on outreach to all the SO/ACs to discuss their specific concerns and seek to create joint activities to mitigate them.

  The RySG DNS Abuse Working Group is currently working on the following agenda items:

  - Continued engagement with OCTO to improve DAAR for the benefit of the ICANN community.
  - Development of DNS Abuse resources that include a framework for the general Internet community to report abuse and for interactions between registries and registrars.
  - Development of DNS Abuse resources with the PSWG to improve engagement between registries and law enforcement.

  Further, in an effort to contribute to community-wide discussions, in 2020 contracted parties provided a clear definition of DNS Abuse. As we note in these comments, it's difficult to successfully discuss and tackle issues that are not clearly scoped and defined. Contracted parties hope that this definition will provide a shared foundation for community discussions.

Comments on the individual recommendations

SSR2 Recommendation 1: Further Review of SSR1 (Priority Low)

1.1. The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 Recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations).

RySG comment**:**

The RySG supports this recommendation.

Identifying and avoiding duplicate work should be an important objective when rationalizing the plan to complete the implementation of SSR1.

SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management (Priority Medium-High)

2.1. ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions.

2.2. ICANN org should include as part of this role's description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position.

2.3. ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach.

2.4. ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, 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 supports these recommendations insofar as they represent strategic requirements for ICANN Org risk management.

We do not support the creation of the new function to oversee security and risk management, as suggested per Recommendation 2.1., as we believe that these roles can (and currently are being) handled by existing members across different functional areas within ICANN Org, including OCTO.

One area of concern is Recommendation 2.4 where it seems to suggest that the CSO role should be required to sign off on all security related contractual terms, including registry and registrar agreements. The RySG notes that Section 7.7 of the Registry Agreement has explicit provisions regarding the renegotiation of the agreement and the implementation of this recommendation must take care not to violate those provisions. ICANN Org also has a history of including the appropriate members of the organization in contractual discussions with contracted parties, and as such there is no need for the SSR2 RT to explicitly include this responsibility in Recommendation 2.4.

SSR2 Recommendation 3: Improve SSR-related Budget Transparency (Priority High)

3.1. The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually.

3.2. The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN strategic plan goals and objectives. ICANN org should implement those mechanisms through a consistent, detailed, annual budgeting and reporting process.

3.3. The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle.

RySG comment**:**

The RySG supports the recommended actions to improve SSR-related budget transparency, but cautions that briefings to the ICANN community on SSR strategy and projects should be high level and not disclose specific security practices, so as not to introduce potential attack vectors.

We reiterate that, as per our previous comment, we do not support the creation of the Executive C-Suite Security Officer referred to in Recommendation 3.1, as this role is already sufficiently being covered within ICANN Org.

SSR2 Recommendation 4: Improve Risk Management Processes and Procedures (Priority High)

4.1. ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them.

4.2. ICANN org should adopt and implement ISO 31000 "Risk Management" and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures).

4.3. ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-Suite

Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications).

RySG comment**:**

The RySG is generally supportive of risk mitigation management within ICANN and believe that this can be sufficiently addressed within the current ICANN staff structures without the addition of a C-Suite level position.

SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (Priority High)

5.1. ICANN org should implement an ISMS and be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement.

5.2. Based on the ISMS, 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.

5.3. ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers.

5.4. ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes to manage risk, security, and vulnerabilities.

RySG comment**:**

We recommend that the Board seek additional clarity from the SSR2 RT regarding what entities "beyond" the ICANN community ICANN Org should report out regarding its security activities.

SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency (Priority High)

6.1. ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs.

6.2. ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.

RySG comment:

While the RySG supports its members adopting vulnerability disclosure policies as good business practice, it does not support ICANN acting as a clearinghouse, gatekeeper, or regulator of vulnerability disclosure policies.

Many RySG members do not operate just as registry operators. For example, dotBrands operate separate and distinct businesses unrelated to their registry. It is unreasonable to expect brands to disclose any vulnerabilities that they handle in the ordinary course of their business to ICANN, and out of ICANN's remit to review the operational processes of brands. The RySG also has concerns about supporting the recommendation to implement such practices in contracts without knowing what specific practices the Review Team has in mind and without following the appropriate and limited processes for amending Registry Agreements.

We would like to remind the Board, when considering this recommendation, that contractual changes can only be effected via contractual negotiations or Consensus Policies.

SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (Priority Medium-High)

7.1. ICANN org should establish a Business Continuity Plan For all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.

7.2. ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., 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. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO).

7.3. ICANN org should also establish a DR plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031.

7.4. ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org.

7.5. ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans.

RySG comment:

The RySG fully recognises the importance of Business Continuity (BC) and Disaster Recovery (DR) processes and procedures.

BC and DR should be based on an inventory of critical systems and an expectation of the level of service to be provided. While the RySG supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan, the proposed scope of "all the systems owned by or under the ICANN org purview" is too broad, contrary to best commercial practice, and thus inappropriate.

BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes. Similar, for example, to the IANA risk management strategy for its services.

We recommend that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators.

SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties (Priority Medium)

8.1. ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the DNS for end-users, businesses, and governments.

RySG comment**:**

Recommendation 8 is not consistent with the terms of the Registry Agreement and must be rejected.

Section 7.7 of the Registry Agreement is the section that allows for the bilateral negotiation of a contemplated change to the Registry Agreement between Registries and ICANN itself, not third parties that are not a party to the Agreement, with one exception: The Registry Agreement considers the possibility of a "Working Group" that may participate in these negotiations, but it is explicitly the registries that makes such an appointment, not ICANN. (See 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."). It should also be noted that the Registry Agreement explicitly states that there are no third-party beneficiaries to the Registry Agreement. (Registry Agreement, Section 7.8).

SSR2 Recommendation 9: Monitor and Enforce Compliance (Priority High)

9.1. The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse-related obligations in contracts, baseline agreements, temporary specifications, and community policies.

9.2. ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org.

9.3. ICANN org should have compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans.

9.4. ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.

RySG comment**:**

The implication of Recommendation 9 is that ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement. The Registries disagree with this characterization and note that Registry Operators' compliance with their abuse obligations were recently audited[2] by ICANN Compliance.

In our comments on the Draft Report Recommendation 10, the RySG made it very clear that any recommendations regarding ICANN's Compliance functions should be linked to specific contractual terms and tied to a specific problem statement. As such, we are disappointed to see that Recommendation 9.1 remains extremely vague, and we reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars. Such a recommendation exceeds the scope of this Review.

SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms (Priority High)

10.1. ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct— ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse- related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication.

10.2. Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.

10.3. Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page.

RySG comment**:**

As mentioned before in this comment, the RySG agrees on the importance of clarity in terminology and definitions around DNS Abuse. However, we stress that any discussion around a definition of DNS Abuse in the ICANN context must bear in mind ICANN's remit as outlined in the Bylaws. A resulting definition cannot exceed the Bylaws.

[2] 'Contractual Compliance Report on Registry Operator Audit for Addressing DNS Security Threats', ICANN, 17 September 2019, https://www.icann.org/en/system/files/files/contractual-compliance-registry-operator-audit-report-17sep19-en.pdf

This said, the RySG would welcome a culture of open discussions aimed at further evolving the definitions of DNS Abuse in the future, as suggested in Recommendation 10.2. We would, however, recommend acknowledging the traditional stakeholders in a CCWG, including Contracted Party representatives, in the recommendation, in addition to the stakeholders named. As noted in these comments, Contracted Parties have worked to establish a definition of DNS Abuse as part of existing community efforts and discussion.

SSR2 Recommendation 11: Resolve CZDS Data Access Problems (Priority Medium)

11.1. The ICANN community and ICANN org should take steps to ensure that access to Centralized Zone Data Service (CZDS) data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials.

RySG comment**:**

In our comment on the Draft Report, the RySG voiced concerns with the inclusion of this recommendation because the current system for access to CZDS data not only provides sufficient access but was also the result of lengthy negotiations taking into account the varying needs of different members of the ICANN community, including the registries that provide this access. We continue to believe that this recommendation is both superfluous and out of scope.

The current CZDS requestors are required to create an ICANN Account and provide their Organization Name, Address, City, Country Code, Contact Phone, and Contact Fax. This information must be verifiable by the Registry Operator. Requestors must also agree to the Terms of Use.

The current credentialing requirements also aim to protect against the zone file data being misused as attack vectors. For example, the Registry Agreement Spec 4 section 2.15 requires that in the Terms of Use the requestor is not permitted to use zone file data to interrupt, disrupt or interfere with the normal business operations of any registrants. So, while zone file data can be used by anti-crime organizations, businesses, cybersecurity professionals, law enforcement, and researchers to combat DNS Abuse, there is also scope for the zone file data to be misused to disrupt legitimate business activities. The current CZDS requirements reflect a balance between ease of access to zone file data, and responsible registry practices to ensure that requestors are accountable for their use of zone file data.

SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review (Priority Medium)

12.1. ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities.

12.2. ICANN org should structure its agreements with data providers to allow further sharing of the data for non- commercial use, specifically for validation or peer- reviewed scientific research. This special no-fee non- commercial license to use the data may involve a time- delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN website. ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting.

12.3. ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports.

12.4. ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS.

RySG comment**:**

The RySG objects to this recommendation set as it lacks a statement of what problem it is trying to solve. ICANN Org has produced DAAR as a means of informing the community of the apparent existence of DNS Abuse. There are other organizations that produce similar types of reports within the context of their own mission and purpose.[3] The RySG's DNS Abuse Working Group (and its predecessor the DAAR Working Group) has been working collaboratively with OCTO to ensure that DAAR provides the community with the best information available. Without a stated objective or observable problem this recommendation prescribes a solution with dubious value.

Specifically, the notion of a time-delay in data-sharing is antithetical to the goal of mitigating abuse as quickly as practical and would appear to be competitive with ICANN Org's compliance responsibilities that also occur after-the-fact.

Also, in our comments on the Draft Report, we objected to Recommendation 12.3 (13.1.1 in the Draft Report), noting that publishing lists of Registries and Registrars whose domains have been targeted for perpetrating security threats does not accomplish the goal of curbing or decreasing actual instances of DNS abuse. The fact is that neither Registries nor Registrars control the source of most DNS abuse and thus the quantity of alleged DNS abuse is not actionable by itself. The Final Report again fails to make a compelling argument for how publishing such information will have a meaningful impact on the overall levels of DNS abuse.

SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting (Priority High)

13.1. 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 an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all generic top-level domains (gTLDs); the participation of each country code top-level domain (ccTLD) would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.

13.2. ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS.

RySG comment**:**

The RySG has serious concerns about the quality of the output of the proposed solution.

[3] The APWG has been producing a Phishing Activity Trends Report every quarter https://apwg.org/trendsreports/ for many years.

Any such reporting system would need to include a process to qualify the accuracy and legitimacy of the complaints submitted before they are passed on for required action by Contracted Parties or aggregated and published in a report.

SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements (Priority High)

14.1. ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold.

14.2. To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains.

14.3. Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and then issue a notice to the relevant party.

14.4. ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Contractual Compliance should move to the de-accreditation process.

14.5. ICANN org should consider offering financial incentives: contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold.

RySG comment**:**

The RySG does not object to Recommendation 14.2. ICANN does not currently provide registries with the lists of domains that it identifies using DAAR and believes it to be a sensible recommendation that could be a valuable tool to provide contracted parties more data and better enable us to identify alleged DNS Abuse.

The remaining items in Recommendation 14 must be rejected as they would violate the terms of the Base gTLD Registry Agreement (the "Registry Agreement") that govern how temporary policies/specifications may be utilized by ICANN. Specification 1, Section 2 of the Registry Agreement states, in part:

> "Temporary Policies. Registry Operator shall comply with and implement all specifications or policies established by the Board on a temporary basis, if adopted by the Board by a vote of at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the Stability or Security of Registry Services or the DNS… Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives."

Registry Agreement, Specification 1, Section 2. It should also be noted that the terms Stability and Security are not amorphous or generic concepts in the Registry Agreement, but rather are defined terms with restricted meanings.[4]

[4] As stated in the Registry Agreement, Section 7.3:

It should be noted that unlike the call for a temporary specification contained in the SSR2 recommendations, the original Temporary Specification for gTLD Registration Data[5] in 2018 met the contractual requirements for temporary specifications. That Temporary Specification was promulgated immediately prior to the obligations of the European General Data Protection Regulation (GDPR) taking effect, which would have prohibited the disclosure of certainly personally identifiable information in the WHOIS. Contracted parties would have been immediately in a position where compliance with applicable law was mutually exclusive to compliance with the agreements with ICANN. The 2018 Temporary Specification was used in order to *prevent* "the unauthorized disclosure, alteration, insertion or destruction of registry data" in a manner that did not comply with GDPR and was narrowly tailored to achieve that result.

A temporary policy/specification is a contractual tool set forth in the Registry Agreement and the Registrar Accreditation Agreement and is not intended to serve as an end-around to ongoing Community discussion or of the multistakeholder model itself.

Recommendation 14 fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways:

(1) The Recommendation fails to meet the requirement that a temporary specification 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.

Analysis:

(1) <u>The recommended temporary specification is not narrowly tailored, as required by the Registry Agreement.</u>

Recommendation 14 from the SSR2 would violate the contractual requirements for when a temporary policy/specification may be utilized by ICANN. Both the base Registry Agreement and Registrar Accreditation Agreements require that any temporary specification must be *as narrowly tailored as feasible* to achieve its stated goal. <u>See</u> 2013 RAA Spec. 4 § 2.1; Base TLD RA Spec. 1, §2.1

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

"[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]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] Temporary Specification for gTLD Registration Data, https://www.icann.org/resources/pages/gtld-registration-data-specs-en

the legal system.[6] 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.

The Registry Agreement works very similarly with regards to temporary specifications in that 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.

While we understand the SSR2 RT's intent to improve security and stability, the work team admittedly utilized specific outputs like the temporary specification in its report not because it is the narrowly tailored or best way to achieve their goals, but rather because of the administrative way they wanted their outputs structured. In its recent webinar[7], the review team noted it had "a lot of discussion about whether to get very specific about implementations. And the reason where we did that was the SMARTness" relying on the SMART Goal format. The team continued "It's specific, measurable, assignable, relevant, trackable. So, if your goal is to be all of those things, then you'd have to be pretty darn specific about what to do. And so, we tried in the findings to say what we were trying to achieve and then the recommendation providing (sic) all those SMART criteria for a way to get to that point." Using a temporary specification in order to have a consistent format for recommendations is absolutely antithetical to the rigid contractual requirements for use of temporary specifications.

(2) <u>The Temporary Specification must address an immediate need for the protection of the Security and Stability of the DNS and not be used to undermine Community discussions.</u>

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 (Registrar Accreditation Agreement Spec. 4 §2; Registry Agreement Spec. 1, §2). Recommendation 14 fails to meet that requirement in a number of ways. First, the review team has not articulated some new threat to the Security or Stability of the DNS, rather, they describe long standing policy discussions around DNS Abuse that have been ongoing for years within ICANN Community discussions.

The Registry Stakeholder Group takes the issue of DNS Abuse very seriously and continues to take steps to systematically combat DNS Abuse. These steps, combined with other industry led efforts like the Framework to Address Abuse have led to a steady decline of DNS Abuse, as noted by ICANN's own Office of the CTO. During the ICANN69 plenary on DNS Abuse, OCTO noted that over the last three years normalized DNS Abuse rates are going down.[8] Similarly, OCTO noted that the aggregate security threats went down over that same period, stating "the trend over time is going down pretty obviously."[9] In fact, over that time period, the only category of abuse that went up was spam, which as ICANN has previously noted is outside of its remit.[10]

[6] <u>See</u> <u>Duncan v. Becerra</u>, 970 F.3d 1133, 1164 (9th Cir. 2020) (noting that strict scrutiny is the "most rigorous and exacting standard" of review of laws).

[7] https://community.icann.org/display/SSR/WEBINAR:++SSR2+Final+Report+%7C+11+February+2021+@+15:00+UTC

[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.

[9] ICANN, *ICANN69 | Virtual Annual General – DNS Abuse – Transcript*, at 7, available at: https://cdn.filestackcontent.com/content=t:attachment,f:%22I69_HAM-Tue20Oct2020__DNS%20Abuse-en.pdf%22/cNDtDrgmSuWKt34K9NoD.

[10] ICANN, *About Spam*, available at https://www.icann.org/resources/pages/spam-2013-05-03-en .

The Registries understand concern regarding DNS Abuse and agree it is an important issue, which is why we continue to take the steps we do to combat DNS Abuse. This includes the work we accomplished with the Public Safety Working Group in creating the Framework for Registry Operators to Respond to Security Threats[11], which provides helpful guidance for registries in addressing DNS Abuse. Similarly, we worked with ICANN Org to publish the Specification 11(3)(b) Advisory, that explains registry obligations regarding identifying DNS Abuse in a gTLD's registrations. We continue to work on these foundations and have founded the RySG DNS Abuse Working Group. The Registrar Stakeholder Group (RrSG) also has a Working Group dedicated to DNS Abuse related issues. The RrSG DNS Abuse Working Group and RySG DNS Abuse Working Group have kicked off an outreach program to directly hear from other SOs and ACs regarding their concern on DNS Abuse and how the registries and registrars can hopefully be a resource for the Community as we continue our dialogue. The RySG and RrSG DNS Abuse groups have also requested time at ICANN70 to continue these discussions and have an open Question and Answer session between the community and the contracted parties on DNS Abuse. These Working Groups have also begun creating Output documents on specific topics related to DNS Abuse to inform both contracted parties and the broader Community on issues related to DNS Abuse.

These discussions continue in earnest and good faith and we believe they should be allowed to continue. These Community efforts should not be short-circuited by an impermissible temporary specification that would undermine them and the multistakeholder model.

SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements (Priority High)

15.1. After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported Expedited Policy Development Process (EPDP) to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template.

15.2. The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Contractual Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days.

RySG comment**:**

Based upon the RySG's strong objection to Recommendation 14, which would create a Temporary Specification, the RySG also objects to the formation of a related EPDP.

In addition to the objection based upon the RySG's opposition to Recommendation 14, the RySG notes that this recommendation does not meet the requirements for an EPDP and represents an attempt to circumvent the existing policy development process.

[11] Framework for Registry Operators to Respond to Security Threats, available at: https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en

First, 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."[12]

Second, it's the GNSO, not the Board, that determines if these limited conditions have been met and if an EPDP should be initiated.

Finally, in 15.1 and 15.2 the recommendation attempts to predetermine the participation, scope, and outcomes of an EPDP which disregards the role of the GNSO and the policy development process.

SSR2 Recommendation 16: Privacy Requirements and RDS (Priority Medium)

16.1. ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the Registration Directory Service (RDS).

16.2. ICANN org should create specialized groups within the Contractual Compliance function that understand 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 RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems).

16.3. ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches.

RySG comment**:**

As noted in our comments to Recommendation 9 and in our comments to the Draft Report, any recommendation regarding ICANN's Compliance functions should be linked to specific contractual terms and tied to a specific problem statement. We also reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars.

In particular, 16.3 suggests that ICANN Compliance should audit Registry and Registrar compliance with a Registry or Registrar's own internal policies and procedures as opposed to its contractual obligations with ICANN. Such a recommendation exceeds the scope of ICANN Compliance's role to enforce contractual requirements.

SSR2 Recommendation 17: Measuring Name Collisions (Priority Medium)

17.1. ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which

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

controlled interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the appropriate handling of sensitive data and security threats.

17.2. The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion.

RySG comment**:**

The Final Report mentions the work of the Name Collision Analysis Project (NCAP) but fails to explain how that work is distinct from what is being proposed by this recommendation. While the RySG is supportive of the NCAP work, as noted in the overarching comments, we cannot support recommendations that repeat or represent significant overlap with other active work. Absent a clear and compelling problem statement, we urge the Board to reject this recommendation.

SSR2 Recommendation 18: Informing Policy Debates (Priority Low)

18.1. 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 Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior.

18.2. ICANN org should ensure that these reports include relevant observations that may pertain to 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.

18.3. ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS.

RySG comment**:**

In much the same way that ICANN monitors and offers neutral summary reports on legislative developments and identifier technology issues, it is reasonable for ICANN to do so for other topics related specifically to ICANN's mission and scope. However, it is unclear how recommending that ICANN offer an interpretation or analysis (including proposing additional studies) of these third-party efforts by specifically targeting only one part of the ICANN community is within either the Review Team's scope of work or ICANN's.

SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite (Priority Low)

19.1. ICANN org should complete the development of a suite for DNS resolver behavior testing.

19.2. ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained.

RySG comment**:**

The report fails to explain why the development of the DNS Regression Test Suite is a requirement of ICANN Org. Similar to the context for Recommendation 18, it is reasonable for ICANN to track and report on the behavior of DNS resolvers since they are a significant client of the DNS services that registries are required to support. However, the RySG considers making this an obligation or requirement of ICANN out of scope and objects to Recommendation 19.

SSR2 Recommendation 20: Formal Procedures for Key Rollovers (Priority Medium)

20.1. ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for Public Comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process.

20.2. ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the root KSK rollover process.

RySG comment**:**

[no comment]

SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators (Priority Medium)

21.1. ICANN org and PTI operations should accelerate the implementation of new Root Zone Management System (RZMS) security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email.

RySG comment**:**

The RySG is supportive of enhancing security in the Root Zone System and efforts in that direction.

SSR2 Recommendation 22: Service Measurements (Priority Low)

22.1. For each service that ICANN org has authoritative purview over, including root zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and metrics on a single page on the icann.org website, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior).

22.2. ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility.

RySG comment:

The RySG strongly supports Recommendation 22.

SSR2 Recommendation 23: Algorithm Rollover (Priority Medium)

23.1. PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS.

23.2. As a 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.

RySG comment:

[no comment]

SSR2 Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process (Priority Medium)

24.1. ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results.

24.2. ICANN org should make the Common Transition Process Manual easier to find by providing links on the EBERO website.

RySG comment:

[no comment]

Note on Inaccuracy in Section "Unachieved Safeguards for the New gTLD Program

The RySG notes that the date of 2013 referred to in the paragraph beginning "In 2013, ICANN's Competition, Consumer Trust and Consumer Choice (CCT) Review Team reviewed the effectiveness of these safeguards…" is a factual error. The call for expressions of interest for the CCTRT was not issued until October 2015[13], with the first meeting of the review Team being in January 2016. For the sake of having future access to an accurate record, the SSR2 RT should be asked to correct this error.

[13] https://www.icann.org/news/announcement-2-2015-10-01-en; https://community.icann.org/pages/viewpage.action?pageId=58725542 .