The ICANN GNSO "Business Constituency"

# Comment on Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

Status: FINAL

Version: 4

8-Apr-2021

**Business Constituency Submission**

**GNSO//CSG//BC**

**Background**

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter:
The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:

1. promotes end-user confidence because it is a safe place to conduct business
2. is competitive in the supply of registry and registrar and related services
3. is technically stable, secure and reliable.

## BC comment on Final Recommendations for the 2nd Security, Stability, and Resiliency Review (SSR2)

The Business Constituency is pleased to comment on the SSR2 Report and thanks all members of the Team for their excellent work with the review assignment.[1]

Under ICANN Bylaws (Section 4.6(c)):

> *The Board shall cause a periodic review of 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 ("SSR Review").*

The BC strongly supports this review process and the productive suggestions it has yielded, in both SSR1 and SSR2. It now is critical that the Board accept SSR2 recommendations as documented and take responsibility for driving expeditious and effective implementation of all recommendations.

The SSR2 Review Team offered 24 groups of recommendations, resulting in 63 specific recommendations, starting with the evaluation of ICANN org's response to the SSR1 recommendations. To add specificity that may have been lacking in the team's SSR1 endorsements, the team broke those groups of SSR2 recommendations down into detail; the recommendations were then structured to offer insight on internal ICANN org operations, ICANN org's engagement (particularly contracts and complaint handling), and how ICANN org can take steps to both improve its own SSR actions and help others understand how to improve theirs.

ICANN should note that recommendations throughout the document often influence each other and have interdependencies. ICANN Org and Board should take this into account when developing implementation plans. Finally, it is commendable that the review team reached full consensus on every recommendation.

**General Comment**

The BC must again comment regarding its -- and the community's -- disappointment in the Board's refusal to oversee timely implementation of previous reviews, including SSR1. The independent review process demands tangible results, and not simply reports that sit idle.

[1] ICANN public comment page at https://www.icann.org/public-comments/ssr2-final-report-2021-01-28-en

The BC commented on the draft SSR2 report in March 2020 and would like to reiterate those comments for the full report[2]. In addition, the BC makes the following general comment.

As the report indicated, ICANN's implementation of the SSR1 report was largely partial and can be estimated to be at about 30-40% of total recommendations, which is unacceptable to the BC. The BC notes that the SSR2 team did a thorough job of reviewing the implementation of SSR1 recommendations and aligned its own recommendations to support (and measurably improve) the SSR1 report. The BC now recommends ICANN Org focus on full implementation of SSR2 recommendations, which are inclusive of matters not implemented from SSR1.

**Specific Comments**

**Recommendation 1:**

The BC does not favour an unending cycle of reviews that are occupied by measuring implementation of prior recommendations. As such, we strongly encourage ICANN and the community to turn their attention to implementation of *all* outstanding recommendations. Therefore, the BC thinks Recommendation 1 may be unnecessary.

When it comes to a clear and comprehensive SSR policy, ICANN org does not have an overarching strategy or identifiable goals. Without a functional SSR strategy and integrated security and risk management (e.g., policy, procedures, standards, baselines, guidelines), SSR-related responsibilities are not assigned, measured, and tracked, leading to a lack of transparency and accountability. The BC urges the ICANN Board to act on this gap as a matter of priority.

To address the operational challenge of full implementation of the SSR1 report, the BC agrees that creation of a C-suite position is warranted, with that position responsible for both Strategic and Tactical Security and Risk Management. Further, that role should oversee SSR2 Recommendation 3: Improve SSR-related Budget Transparency for the SSR2 recommendations that expands upon the original SSR1 recommendation.

Noting that there is a nexus between most of the SSR1 recommendations and those of SSR2, the BC posits that measurable recommendations in SSR2 should take care of any need for the Board to conduct another review of SSR1.

Regarding SSR1 Recommendation 19, the SSR2 team wrote:

> "Documentation of the implementation lags very much behind the implementation, so it does not offer the community a way to track the SSR-related activities."

This underlines the importance of appropriate and timely reporting on implementation work; the BC accordingly supports this as an essential element of staff work scope. Therefore, the BC recommends that a time limit be set by the Board for the implementation of all SSR2 recommendations (except Recommendation One, which now is unnecessary).

[2] March 2020 BC comment on SSR2 Draft report, at https://www.bizconst.org/assets/docs/positions-statements/2020/2020_03March_10%20BC%20comment%20on%20SSR2%20Report.pdf

SSR1 recommendations 19, 20 and 25 call for a public dashboard for tracking SSR-related work. The BC agrees and urges ICANN to employ existing and new dashboards more consistently; they remain relevant and are key to successful implementation of SSR2 recommendations 2-24, in particular.

**Recommendations 2-24:**

The BC stands by its previous comments on these recommendations.

Of these earlier comments, we re-emphasize the special importance of **SSR2 Recommendation 7: Improve Business Continuity and Disaster.**

ICANN's lack of a Business Continuity and Disaster Recovery Plan is especially concerning. Hence, SSR2 Recommendation 7 should be **of highest priority.**

The to-be-selected Chief Security/Information Security Officer should maintain an ongoing and frequently updated dashboard report of SSR2-related activities and, further, should publish an annual report. As SSR2-related tasks will be resolved throughout the year, the dashboard should not be a static re-representation of the contents of a report which is issued only once annually.

The BC further highlights the following recommendations as top priority:

Recommendations 4 & 5: **Close internal risks, use common industry standards.** Adopt and implement ISO 31000 "Risk Management" and validate implementation w/ independent audits; implement an ISMS and be audited and certified by third party.

Recommendation 8: **Represent public interest in negotiations w/ contracted parties.** ICANN should commission a negotiating team that includes abuse and security experts (with no connections to 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 security, stability and resilience of the DNS for end-users, businesses, and governments.

**Report contracted party breaches.** The BC agrees with implementation of coordinated vulnerability disclosure reporting on SSR-related issues (*i.e.*, breaches at any contracted party) and prompt communication of critical vulnerabilities to trusted and relevant parties.

Recommendation 9: **Enforce compliance.** The BC agrees with directing ICANN's 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;
- proactively monitor and enforce registry/registrar contracts to improve the accuracy of registration data;
- conduct external audit of compliance activities with public reports and implementation; and
- publish regular reports that enumerate missing tools that would help support ICANN org to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.

Recommendation 10: **Define/act on abuse.** The BC advocates for posting ICANN org's current working definition of DNS abuse (including ICANN's definition as used in projects, documents, and contracts); for use of the definitions consistently in public documents, contracts, review team implementation plans, and other activities; and have such uses referenced in public web page; **create cross-community working group (CCWG)** to establish a process for evolving the definitions of prohibited DNS abuse. We believe this should be done (in no more than 30 business days) at least once every two years, on a predictable schedule; and this group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.

Recommendation 11: **Resolve CZDS Data Access Problems.** Ensure that access to Centralized Zone Data Service (CZDS) data is available in a timely manner and without unnecessary hurdles to requesters.

Recommendation 12: **Overhaul DNS abuse analysis & reporting efforts.** The BC advocates for the publication of reports that identify registries and registrars whose domains most contribute to abuse. Reports should include machine-readable formats of the data, in addition to the graphical data in current reports. Further, ICANN 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; and
- 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.

**Incentivize abuse mitigation.** ICANN 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.

Recommendation 13: **Create central DNS abuse complaint portal.** The BC believes ICANN could establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties (system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata); ICANN also should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS.

Recommendation 14: **Temp Spec on abuse.** ICANN should issue a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting activity as abusive below a reasonable and published threshold. ICANN should further provide contracted parties with lists of domains in their portfolios identified as abusive (in-line with SSR2 Rec. 12.2 regarding independent review of data and methods for block-listing domains); should the number of domains linked to abusive activity reach the published threshold described in SSR2 Rec. 14.1, ICANN would be required to investigate to confirm the veracity of the

data and analysis, and then issue a notice to the relevant party. Contracted parties then would have 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, Compliance should move to the de-accreditation process.

Recommendation 15: **Launch an EPDP for evidence-based security improvements.** After the temp spec, the Board should launch an EPDP to create an anti-abuse policy; EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temp Spec for gTLD Registration Data EPDP team charter as a template.

The BC considers as top priority the expedited implementation of the SSR2 recommendations highlighted above.

---

This comment was drafted by Jimson Olufuye, Mark Svancarek, and Waudo Siganga, with edits by Mason Cole and Steve DelBianco.

It was approved in accord with our charter.