BUSINESS CONSTITUENCY (BC) COMMENT:

SECOND SECURITY, STABILITY AND RESILIENCY (SSR2) REVIEW TEAM DRAFT REPORT[1]

Thank you for the opportunity to comment on this important matter before the ICANN community. The BC further thanks the volunteer efforts of the members of the SSR2 Review Team (RT) for their hard work and their dedication to the ongoing security, stability and resilience of the domain name system (DNS).

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.

Prelude to the report: Overarching comments

The BC supports the recommendations detailed in the report and, further to our longstanding advocacy for mitigating DNS abuse, is pleased to see that many of the RT's recommendations address this problem.

Before setting out its detailed comment on SSR2, the BC highlights here a number of overarching comments for the community, ICANN Org, and the ICANN Board:

- SSR1 recommendations must be fully implemented if SSR2 recommendations are to have full impact. It is mystifying as to why SSR1 recommendations -- which were issued *eight years ago* in 2012 -- have not been put into place, despite ICANN Org's claim to the contrary. (It would be helpful to understand why this is the case; for example, are more resources needed, or has ICANN deprioritized this work in favor of other areas?)
- DNS abuse must be taken seriously. The SSR2 RT has done a commendable job in tailoring recommendations to address abuse-related issues. As the BC has oft advised (in a recent statement and even more recent letter to the ICANN Board), DNS abuse has become an acute issue, one that deserves the community's and ICANN's urgent attention. We therefore note the Review Team's observation (page 31) that "the publications, statements, and related actions by ICANN organization have consistently understated or omitted the impact of systemic abuse of the DNS and its use as a platform for launching systematic attacks on individual and organizational systems worldwide".
- Independent oversight of ICANN efforts cannot be abridged. The BC echoes here its input on the Third Accountability and Transparency Review Team (ATRT3) draft report, where it called specifically for the continuation of meaningful and frequent community review of ICANN actions. The BC believes this accountability mechanism will be critical to the long-term impact and success of the SSR2 RT's recommendations.

[1] Public comment page at https://www.icann.org/public-comments/ssr2-rt-draft-report-2020-01-24-en

Delinquency in SSR1 recommendation implementation

The SSR2 RT examined each recommendation from the first review team's effort in 2012 and confirmed that nearly all of those recommendations, while still relevant, have *not* been implemented and, in fact, need further attention from the community:

SSR1 Recommendation Overview																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Relevant	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Implemented	P	P	P	P	P	N	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Work needed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y

Y = Yes P = Partial
N = No - = Not applicable

The BC fails to understand why implementation of these recommendations are now eight years delinquent. As is the case with recommendations from the CCTRT and other review teams, ICANN Org and the ICANN Board have delayed or outright ignored community recommendations that would improve the health and stability of the DNS. The BC strongly encourages the ICANN community to demand the implementation of recommendations from both the SSR1 and SSR2 review teams, and for an associated timeline for implementation to be developed and published by ICANN Org. The danger, of course, is that a great deal of thoughtful and impactful work will go to waste without ICANN's action, and that the DNS will be weaker as a result.

SSR2 recommendations and DNS abuse

In the aggregate, ICANN Org and the community have worked on the fringes of DNS abuse matters, but have yet to meaningfully address them with impactful action. The BC therefore is pleased to see the RT emphasizing, via its recommendations, the further need to address DNS abuse. As the Governmental Advisory Committee (GAC) has stated about the importance of addressing DNS abuse, "Protecting the public from security threats and DNS Abuse is an important public policy issue." The BC is hopeful that position is shared across the ICANN community.

As referenced in the above overarching comment, the BC is strongly on record with its advocacy for mitigating DNS abuse. The RT's recommendations 11 through 19 are affirmations of the broader community's support for meaningful action on DNS abuse, and the BC supports these recommendations (further detail below).[2]

The need for independent community oversight

The BC was disappointed to see suggestions from the third Accountability and Transparency Review Team (ATRT3) that would weaken community oversight of ICANN or otherwise unnecessarily introduce bureaucracy. As noted above, if the SSR2 RT's recommendations are to be fully effective, they will need community input, review and cooperation. Accordingly, the BC reinforces here its ATRT3 comment, where it was stated that the BC:

- Does not support a new oversight mechanism to coordinate reviews and implementation work;

2 While not specifically addressed in SSR2 RT recommendations, the BC points out that many domain name registrants either do not have access to or do not understand security measures that are available or should be available to protect their registrar accounts and domain name registrations. Further, few registrars offer registry lock or two-factor authentication services for deterrence of hijacking and unauthorized modifications. ICANN Org should encourage registrars to offer these services by default, and also should encourage education to registrants regarding their use.

- Does not support consolidation of specific reviews (e.g., CCT, SSR, RDS) into a single review conducted every seven years; and
- Supports the addition of three- to five-day workshops for organizational reviews.

The BC went on to say in its same comment:

> *Of particular concern is the systemic problem of ICANN Org failing to implement Board-approved recommendations, even while declaring that all recommendations have been fully implemented. Three review teams -- WHOIS/RDS, ATRT3 and SSR2 -- have recently documented that a significant portion of the previous Specific Review recommendations were not fully implemented, despite staff claims to the contrary. While some Specific Review recommendations certainly could be clearer, it's equally clear that ICANN's Board has not fulfilled its responsibility to ensure their directives are carried out, and that ICANN Org has failed to execute its responsibilities to fully implement all recommendations approved by the Board.*

In this context, SSR2 recommendations stand only to benefit from community oversight (even if only to ensure their implementation), and therefore our position on specific reviews is reiterated.

Addressing vulnerabilities and breaches

In addition to the above overarching comments, the BC wishes to highlight the fact that the SSR2 team has oriented many of its recommendations toward addressing vulnerabilities or potential breaches. While it may be disturbing that ICANN Org has not done enough independently in this realm, the BC is gratified that the RT has made prescient recommendations in the manner that it has.

Please see table on following pages for BC comments on individual recommendations.

Conclusion

The BC strongly encourages the adoption of these recommendations, their timely implementation, and their ongoing review. We again thank the RT for its hard work and sensible recommendations, and thank ICANN for the opportunity to comment on this important issue.

This comment was drafted by Mason Cole, Susan Kawaguchi, Ben Wallis, Roger Baah and Yusuph Kileo. It was approved in accordance with the BC Charter.

BC comment on individual recommendations

Here is the table of the RT's recommendations, with the BC's "ownership" recommendations in the third column and comment in the fifth column.

No.	Recommendation	Recommended Owner	Priority	BC Comment
1	**Complete the implementation of all relevant SSR1 recommendations[3]**	ICANN Org	High	The BC believes this is critical. ICANN Org has incorrectly represented these recommendations as implemented, when in fact practically none are completed. These recommendations are nearly eight years old, and the time has long since passed for their implementation.
2	**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	ICANN Org	High	The BC concurs with this recommendation.

3 For a comprehensive list of SSR1 recommendations, see pp. 65-93 at https://www.icann.org/en/system/files/files/ssr2-review-24jan20-en.pdf.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	international standards (e.g., ITIL, ISO 27001, SSAE-18) for its operational responsibilities.			
3	**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.	ICANN Org	High	The BC concurs with this recommendation.
4	**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	ICANN Org	Medium	The BC concurs with this recommendation. Budget transparency would provide a clear indicator of ICANN Org's prioritization of SSR-related recommendations. However, the BC disagrees with the concept that ICANN may be less transparent according to level of effort involved, as a subjective determination -- ICANN

No.	Recommendation	Recommended Owner	Priority	BC Comment
	performing SSR-related functions, including those associated with the introduction of new gTLDs.			must strive for transparency throughout each of its processes.
5	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).	ICANN Org	High	The BC concurs with this recommendation.
6	**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.	ICANN Org	High	The BC concurs with this recommendation and further recommends this position be installed as an executive at the C-level of ICANN.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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.			
7	**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. 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).	ICANN Org	High	The BC concurs with this recommendation. In particular, the BC agrees with the recommendation regarding measurement. Too often, ICANN does not benefit from measurement data that could help mitigate abuse, improve processes, inform policymaking, or otherwise assist the community. The BC concurs with the RDS2 RT's previous recommendation that all new policies include tracking metrics to understand the policy's efficacy; measurement of success, therefore, is an important part of the SSR2 RT's recommendation here. ICANN should endeavor to source these metrics internally rather than soliciting less-than-reliable, self-reported information from the community.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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."			
8	**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." 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.	ICANN Org	High	The BC concurs with this recommendation.
9	**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.	ICANN Org	High	In general, the BC supports Recommendation 9. However, we suggest ICANN should develop and manage an ISO 22301 Business Continuity Management Systems (BCMS), which clearly indicate regular testing of disaster recovery sites and publishing test results within a specified period to all stakeholders as required. The BC also suggests regular internal auditing to prepare adequately for external audits and certification. We also recommend that the implementation team undergo individual certification in ISO

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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.			22301/ISO 27031 Implementation and Lead Auditor (I & L.A) program to prepare them in the efficient implementation of Business Continuity Plan (BCP).
10	**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. 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 to closure and passing and implementing a WHOIS policy in the year after this report is published.	ICANN Org, ICANN Board	High	The BC concurs with this recommendation and encourages both staff and the Board to take active roles in their implementation. ICANN's compliance function needs improvement, both in the manner in which it is staffed and in the tools it has available to correct problematic behavior on the part of contracted parties or their customers. This recommendation, correctly implemented, would have a lasting impact on ICANN Org's capability to address abuse and ensure security and resilience. The BC further agrees with the specific recommendation about bringing the EPDP to a close and implementing WHOIS policy. All parties need and deserve the predictability that will come with a fully implemented policy.

No.	Recommendation	Recommended Owner	Priority	BC Comment
11	**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. 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 Communique10 and for Specification 11), and addressed in international conventions such as the Convention on Cybercrime and its related "Explanatory Notes"—to use in conjunction with ICANN org's DNS Abuse definition. 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.	ICANN Org, ICANN Board	High	The BC concurs with this recommendation and reiterates its previous statements regarding DNS abuse: • …while the BC appreciates the need for actionable definitions of abuse, we are concerned about recent efforts to limit or otherwise over-restrict discussion about the serious issue of domain name system abuse. Such a subject deserves fulsome consideration by the entire community… • ICANN has a responsibility to enforce its contracts in the areas of DNS-related abuse. This community dialogue cannot delay or defer ICANN's commitments or operations related to DNS abuse. • ICANN should clarify the purposes and applications of "abuse" before further work is done to define DNS abuse. • Once those purposes are identified, ICANN should determine whether abuse definitions used by outside sources can serve as references for the ICANN community, or whether a new, outcomes-based nomenclature could be useful (including impersonation, fraud, or

No.	Recommendation	Recommended Owner	Priority	BC Comment
				other types of abuse) to accurately describe problems being addressed.
12	**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.	ICANN Board	High	The BC concurs with this recommendation but also initially encourages ICANN to begin with proactive review of registrar compliance with the Temp Spec. The Compliance team could start with review of redaction of data, easy-to-find reveal request policies on registrar websites and average response time to requests for registrant data.
13	**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 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	ICANN Board, ICANN Org	High	The BC concurs with this recommendation. The DAAR program is one of unrealized potential. Executed well, DAAR would have the capability of informing ICANN (and the community) with precision regarding the source(s) of abusive behavior, making it easier to enlist the cooperation of contracted parties in mitigation efforts. The BC encourages ICANN Org to invest further in an improved and robust DAAR program, and encourages the ICANN Board to lend its support and oversight to the effort. We note the 13.1.1. recommendation to publish DAAR reports in a way that "identifies registries and registrars whose domains most contribute to abuse according to the DAAR methodology". We recommend going further than that in expanding the detail of the public DAAR reports to report activity by registry, by registrar and by measured security threat.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	advisory activities that would enhance domain name abuse prevention and mitigation.			
14	**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, analyze, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse.	ICANN Org	High	While the BC historically has discouraged ICANN Org from engaging on matters of pricing, this data could be informative and helpful in identifying and targeting sources of DNS abuse. The BC supports.
15	**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. 15.2. 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). 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.	ICANN Org, ICANN Board	High	The BC concurs with this recommendation. The BC underlines its previous comments (dating back to input on the CCT review team's findings in late 2018) regarding the establishment of thresholds of abuse harboring and a corresponding instigation of compliance inquiries. The BC believes the problem of abuse is acute enough, and growing fast enough, to warrant such a system, and encourages the contractual changes. For the same reason, the BC agrees with recommendation 15.2 regarding contract termination. With regard to the suite of recommendations under 15.3, the BC concurs here as well -- particularly 15.3.1. The European Union's (EU) General Data Protection Regulation (GDPR) has decimated the investigatory value of the Whois database. The BC reiterates its many inputs calling for sensible access to non-public Whois data, with vigorous enforcement of that access right given to ICANN as a compliance matter.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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.			15.4 also is a particularly useful recommendation in that it seeks to codify in contracts the necessity of addressing DNS abuse as the serious matter that it is. While the BC has applauded the several contracted parties who voluntarily have adopted a framework for addressing abuse, the situation unfortunately requires assertive mandates as a way of truly rooting out abuse.
16	**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.	ICANN Org, ICANN Board	High	The BC applauds this common sense recommendation and encourages ICANN Org and the Board to institute incentive policies as a matter of priority.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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.			
17	**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.	ICANN Org	High	The BC concurs with this recommendation.
18	**Ensure that the ICANN Compliance Activities are Neutral and Effective**	ICANN Board, ICANN Org	High	The BC concurs with this recommendation.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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.			For too long, ICANN's compliance function has been notoriously weak. The BC supports the Board's investiture of additional power into Compliance, and further supports greater accountability by Compliance through the adherence to SLAs. If ICANN is to do its part in mitigating DNS abuse, it must have an effective, accountable compliance function; further, to ensure activities are effective, ICANN's contracts with registries and registrars must be in order and enforceable by compliance.
19	**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.	ICANN Org	High	The BC concurs with this recommendation. ICANN Org should acknowledge and track the rise of misleading naming and trademark infringement as a growing trend in abusive naming. It has long been recognized that most trademark infringement targets users of famous brands and defrauds the individual user, not the large global brand. Abusers recognize the ease with which they can utilize the goodwill of a brand to lead the user to trust the infringer and provide personal information or funds to the abuser.

No.	Recommendation	Recommended Owner	Priority	BC Comment
20	**Complete Development of a DNS Regression Testing** 20.1. ICANN org should complete the development of a suite for DNS regression testing. 20.2. ICANN org should ensure that the capability to perform functional testing of different configurations and software versions is implemented and maintained.	ICANN Org	High	The BC concurs with this recommendation.
21	**Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers** 21.1. ICANN org should implement the recommendations from SAC063 and SAC073 in order to ensure the SSR of the KSK rollover process. 21.2. 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, FSM) for public comment, and community feedback should be incorporated. 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 lessons learned can be used to adjust the process. 21.3. 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.	ICANN Org	High	The BC concurs with this recommendation.
22	**Establish Baseline Security Practices for Root Server Operators and Operations** 22.1. ICANN org, in close cooperation with RSSAC and other relevant stakeholders, should ensure that the RSS governance model as proposed by RSSAC037 includes baseline security best practices for root server operators and operations in order to minimize the SSR risks associated with root server operation. These best	ICANN Org	High	The BC concurs with this recommendation.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	practices should include change management, verification procedures, and sanity check procedures. 22.2. ICANN org should also develop relevant KPIs to measure the implementation of these best practices and requirements and ensure yearly public reporting on how Root Server Operators (RSOs) and other relevant parties, including ICANN org, can meet these KPIs. 22.3. ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as LRoot, and should encourage other RSOs to do the same. 22.4. ICANN org should ensure that the IMRS uses a vulnerability disclosure process (not necessarily public), security reports and intelligence, and communication with researchers and RSSAC advice or recommendations, where applicable.			
23	**Accelerate the Implementation of the New-Generation RZMS** 23.1. ICANN and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes. 23.2. ICANN org should launch public comment as soon as possible on changes regarding revisions to the RZMS policies.	ICANN Org	High	The BC concurs with this recommendation.
24	**Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems** 24.1. ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over.	ICANN Org	Medium	The BC concurs with this recommendation.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	24.2. ICANN org should publish a directory of these services, data sets, and metrics on a single page on the ICANN org web site, such as under the Open Data Platform. 24.3. ICANN should publish annual and longitudinal summaries of this data, solicit public feedback on the summaries, and incorporate the feedback to improve future reports. 24.4. For both sets of KPIs, ICANN org should produce summaries over both the previous year and longitudinally, request and publish a summary of community feedback on each report and incorporate this feedback to improve follow-on reports.			
25	**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: *"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.*	ICANN Org, ICANN Board	High	The BC concurs with this recommendation.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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.*			
26	**Document, Improve, and Test the EBERO Processes** 26.1. ICANN org should publicly document the ERERO processes, including decision points, actions, and exceptions. The document should describe the dependencies for every decision, action, and exception. 26.2. Where possible, ICANN org should automate these processes and test them annually. 26.3. ICANN org should publicly conduct EBERO smoke-testing at predetermined intervals using a test plan coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results. 26.4. ICANN org should improve the process by allowing the gTLD Data Escrow Agent to send the data escrow deposit directly to the EBERO provider.	ICANN Org	High	The BC concurs with this recommendation.
27	**Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers** 27.1. PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security.	ICANN Org	Medium	The BC concurs with this recommendation.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	27.2. As root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.			
28	**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.	ICANN Org, ICANN Board	Medium	The BC concurs with this recommendation.
29	**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	ICANN Org	High	The BC concurs with this recommendation.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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. 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.			
30	**Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates**	ICANN Org	Medium	The BC concurs with this recommendation.

No.	Recommendation	Recommended Owner	Priority	BC Comment
	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.			
31	**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.	ICANN Org	High	The BC concurs with this recommendation.