8 April 2021

RrSG Response to the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

The Registrar Stakeholder Group (RrSG) is pleased to comment on the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report. In addition to the feedback in this comment, the RrSG reiterates the comments it made in response to the SSR2 Review Team Draft Report[1] (to the extent those comments were not incorporated into the Final Report).

While the RrSG appreciates the significant effort of the Review Team in undertaking this important initiative, the RrSG has serious concerns about a number of the recommendations that are contrary to ICANN's bylaws, the Generic Names Supporting Organization (GNSO) Operating Procedures, the Registrar Accreditation Agreement (RAA), the Registry Agreement (RA), and ICANN's bottom-up multistakeholder process. Before providing feedback for specific recommendations, the RrSG would like to provide some general feedback regarding the entire Final Report.

First, the RrSG notes that the final Review Team does not appear to contain any representatives from the RrSG, the Registry Stakeholder Group (RySG), the Internet Service Providers and Connectivity Providers Constituency (ISPCP), and the Not-for-Profit Operational Concerns Constituency (NPOC), and some of the recommendations appear to be significantly biased against the interests of these constituencies. The absence of constituencies is not a justification for creating a Final Report that will significantly (and negatively) impact those constituencies. Some of these constituencies (including the RrSG and the RySG), provided strong comments against or outright disagreement (based upon the RAA or RA) with some of the recommendations in the Draft Report. Much of this feedback appears to be largely ignored, despite Appendix H repeatedly indicating that the feedback was incorporated into the Final Report. The RrSG strongly cautions the ICANN Board against adopting many of the recommendations in the Final Report, and recommends that the Board only approve recommendations that have the full support of the entire ICANN community.

Second, a number of the recommendations include specific instructions to ICANN to change the RAA and the RA. The RrSG notes that these recommendations are contrary to the negotiation process identified in the RAA (Section 7.4), and the RA (Article 7.7), and should be completely rejected by the ICANN Board. The negotiation process is solely between ICANN and the respective contracted parties, and not subject to community initiative, feedback, comment, or approval, despite the conclusions of a Review Team (which as previously noted, did not include any registrar or registry participation). RAA and RA contract negotiations can be a detailed and time-consuming process - the negotiations to replace whois with RDAP in the RAA and RA are still ongoing after eighteen months. Additionally, a number of the recommended changes to the RAA and RA are not technically or commercially feasible, nor is there sufficient justification to support such drastic changes (especially without the participation of the contracted parties).

Third, these recommendations appear to have been made without any consideration of how ICANN org will pay to implement the recommendations - either through additional funding or reprioritization within the existing budget. The RrSG notes that the vast majority of ICANN's budget is ultimately paid by domain name registrants, and the Final Report does not fully explain why registrants should bear this additional burden. In addition to the various initiatives

[1] https://mm.icann.org/pipermail/comments-ssr2-rt-draft-report-24jan20/2020q1/000009.html

and programs recommended in the Final Report, recommendation 13 references an abuse complaint portal. ICANN Org recently estimated that the cost to implement the Standardized System for Access/Disclosure (SSAD) will be approximately $9 million, and a further $9 million annually to operate. The cost of an abuse portal will likely be similar, and without any consideration of these costly initiatives, the ICANN Board should not approve these recommendations.

Fourth, a number of these recommendations cover items that ICANN org is already dedicating significant resources- including the responsibilities of the Office of the Chief Technology Officer (OCTO) and Contractual Compliance. The RrSG struggled to consider recommendations that are duplicative of longstanding ICANN activities, which additionally led the RrSG to question the Review Team's other recommendations, which might be colored by a misunderstanding of the issues, data, and current contracted party abuse initiatives.

For the ease of review, the RrSG's comments are presented in the table below along with the corresponding recommendations.

	Recommendation	RrSG comment
1	**SSR2 Recommendation 1: Further Review of SSR1** 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	1.1. The RrSG generally supports this recommendation.
2	**SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management** 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.	2.1. The RrSG notes that ICANN already has a Chief Security, Stability & Resiliency Officer- John Crain. It is not clear why this recommendation is needed in light of Mr. Crain's significant individual and team contributions to the security and stability of the Internet. 2.2. It is the understanding of the RrSG that through OCTO generally, and John Crain specifically, ICANN already performs these functions.

	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.	2.3 It is not clear to the RrSG how these roles and functions are not already being provided by various ICANN org and IANA staff. This recommendation appears to be redundant and thus the RrSG does not support adopting this recommendation. 2.4. The RrSG notes that the 2013 RAA makes no references to security-relevant items in the RAA, and it is inappropriate for a Review Team (without the participation of anyone in the RrSG) to suggest that such clauses are desirable or practical. It is not the purview of the Review Team to dictate who within ICANN Org shall perform what functions, including the review and approval of any changes to the RAA. While such individual(s) may be consulted, ultimately it is up to the ICANN Org negotiating team (including the participation of ICANN Legal) to approve any terms on behalf of ICANN.
3	**SSR2 Recommendation 3: Improve SSR-related Budget Transparency** 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	3.1. It is not clear from the Final Report how OCTO's current participation in the ICANN community, the Internet community in general, as well as existing OCTO publications are deficient. Specifically, OCTO publishes a number of reports authored by OCTO staff, ongoing research by the OCTO team, and Commissioned Documents. This is only a representative sample of the extensive activities conducted by the OCTO team (additional details are available at https://www.icann.org/octo). Before adopting this recommendation, the RrSG recommends that the ICANN Board consider existing (and significant) ICANN org activities. 3.2. It is not clear to the RrSG how the current cadence of reports and substantial ICANN event participation by OCTO is deficient, and why the Review Team has designated this a high priority item.

	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.	3.3. It is not clear to the RrSG how ICANN's current public comment on its budget (including SSR-related items) and strategic planning is deficient to necessitate this recommendation, nor why the Review Team designated this as a high priority item.
4	**SSR2 Recommendation 4: Improve Risk Management Processes and Procedures** 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).	4.1. The goal of this recommendation is not clear to the RrSG, and thus does not support this recommendation 4.1. 4.2. The RrSG generally supports this recommendation, with the understanding that it will be narrowly tailored, specifically focused, and necessary to achieve the goals of the recommendation. 4.3. As of the date of this comment, ICANN's Office of the Chief Technology Officer (OCTO) comprises approximately 20 staff. It is not clear to what extent the functions identified in this recommendation are not currently performed by OCTO, or why a new position is required to perform these functions. To the extent these functions are not currently performed by OCTO, the team should be capable of incorporating these items into their existing departmental structure.
5	**SSR2 Recommendation 5: Comply with**	As indicated in the RrSG comment to Draft Report,

	Appropriate Information Security Management Systems and Security Certifications 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.	the RrSG generally supports certification, auditing, and reporting of ICANN.
6	**SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency** 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.	6.1. The RrSG does not support this recommendation, for the reasons specified above in the general comments. Additionally, it is not the role of ICANN or the ICANN community to dictate the operational obligations of contractual parties- especially without the participation, agreement, and approval of the contracted parties. The RrSG recommends that the ICANN Board reject this recommendation 6.1 entirely. 6.2. Reporting data breaches to ICANN is already a

	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.	requirement in the Section 3.20 of the RAA. ICANN Compliance has the data/metrics to report on this. Additionally, it is extremely difficult for ICANN to effectively anonymize metrics due to the geography of the contracted parties. Some jurisdictions, such as the United States and China, include a large number of contracted parties so anonymization is possible. Other regions (such as Africa) or countries (such as Ireland), contain only a handful (at most) contracted parties so “anonymized” metrics could easily be reversed engineered to determine the underlying contracted part. To the extent that this recommendation contemplates changes to the RAA, the RrSG reiterates its previous general objection regarding contract modification via Review Team, and urges the ICANN Board to reject this recommendation.
7	**SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures** 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	Although the RrSG is generally supportive of this recommendation, it will defer to IANA regarding whether or not to create and maintain a KSK ceremony location outside of the 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.	
8	**SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties** 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.	8.1. As referenced in the RrSG general comment, this is not acceptable and a violation of the RAA. RAA negotiations are conducted solely as specified in Section 7.4 of the RAA. No matter how desirable to the limited interests in the Review Team, it cannot overrule established requirements in the RAA.
9	**SSR2 Recommendation 9: Monitor and Enforce Compliance** 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	9.1. ICANN Contractual Compliance already performs this function through complaint processing, reviews, and audits. It is not clear to the RrSG what problem this recommendation is intended to fix. 9.2. ICANN Compliance already proactively monitors compliance through audits and review, and additionally in light of complaint processing, does this. Regarding validation of address fields, the RrSG notes that the Across-field Address Validation Working Group (AFAV) is currently paused in light of concerns over GDPR, and additionally that global solution that includes lesser served regions has not been identified. This recommendation is thus premature. ICANN Contractual Compliance already reviews accuracy

	data to ICANN org.	of registration through complaint processing, and prior to GDPR, ICANN org conducted periodic WHOIS Accuracy Reporting System (ARS) reviews. The most recent WHOIS ARS report (June 2018) determined that 98% of domain names have an operable email address or telephone number. It is not clear what the accuracy reviews intend to address. Regarding the arbitrary selection of 50 complaints as a trigger for additional compliance review, the RrSG rejects this arbitrary determination as it fails to incorporate proportionality. For example, while 50 complaints might be substantial for a registrar with only 10,000 domains under management (DUM), it is an insignificant number for a registrar with 10 million (DUM). Failure to appreciate this basic understanding of sampling leads the RrSG to question other recommendations in the Final Report. Finally, it is not the role of the ICANN community to instruct an independent Contractual Compliance department how to conduct its activities.
	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.	9.3. Any audit of Contractual Compliance should focus on its structure, staffing, activities, systems, processes, and the overall efficiency and effectiveness of this function. Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing.
	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.	9.4. As part of ongoing collaboration between the RrSG and ICANN Contractual Compliance, the RrSG has requested ICANN Contractual Compliance make its needs for additional tools known to the RrSG on several occasions. The RrSG is not aware of any specific recommendations from ICANN Contractual Compliance. Additionally, the RrSG supports an independent Contractual Compliance team that does not react to instructions from a Review Team.
10	**SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms** 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	10.1. It is not clear why the Review Team has made this recommendation. This recommendation implies that ICANN is not already doing all of the

	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.	activities within the recommendation, whereas these activities are already ongoing. For example, ICANN already has a working definition of DNS abuse (see https://www.icann.org/octo-ssr/daar), and already tracks and reports on DNS abuse levels on a monthly basis. Additionally, it is very easy to review the RAA and the RA to determine the existing contract language regarding abuse. This recommendation is superfluous and duplicates existing ICANN efforts. 10.2. The formation of a CCWG as described in this recommendation is outside of the ICANN Bylaws and the GNSO Operating Procedures. Additionally, the directions are overly prescriptive, do not allow for realistic timelines, and do not clearly state the problem that the recommendation is attempting to solve. The fact that the recommendation fails to include registrars and registries as participants (the very parties that would be bound by any outcome) reveals that this recommendation is solely intended to dictate additional obligations on contracted parties without their very participation in the process. For these reasons, the ICANN Board should completely reject this recommendation. 10.3 This oblique reference is likely referring to the definition of "abuse" from the 2012 RAP WG Final Report. It is not clear why this was not articulated directly in the SSR2 Final Report. The definition of abuse from the 2012 RAP WG Final Report is a reasonable definition of abuse broadly but not of DNS Abuse specifically. This is, in fact, directly stated by the same report, which stated that "understanding and differentiating between domain registration abuses and domain use abuses is essential in the ICANN policy context, and a failure to do so can lead to confusion."
11	**SSR2 Recommendation 11: Resolve CZDS Data Access Problems** 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	The RrSG does not have a position on this recommendation.

	unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials.	
12	**SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review**	
	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.	12.1. ICANN already operates the DAAR, and it is not clear what limitation or oversight this recommendation intends to address. Without identifying the specific deficiencies, the Review Team should not instruct ICANN to spend significant money to accomplish unidentified goals. The RrSG recommends that the ICANN Board reject this recommendation.
	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.	12.2. It is not clear what issue this recommendation is attempting to address. Before recommending changes to the DAAR, the Review Team should specify the exact problems it is trying to address. Additionally, there is potentially a significant amount of personal and/or confidential data within the DAAR, and it is not clear to the RrSG how the data sharing contemplated in this recommendation will comply with applicable privacy laws in California, the EU, and elsewhere. The RrSG is also concerned how ICANN will offset the cost of this service, as this recommendation implies the use of the data at no cost.
	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.	12.3. To the extent that a registrar or registry receives a notice of breach regarding abuse, then this information can be reported by ICANN Contractual Compliance publicly. Otherwise, this recommendation includes a number of unresolved questions: how will abuse be measured? What abuse will be measured? How is “most contribute” defined? What harm should be considered? The recommendation also implies that the domains belong to registries or registrars, rather than the registrants who use the services and then host a domain name elsewhere. There is also a concern that such “naming and shaming” will lead to contracted parties gaming their numbers to not appear on the list, and further ostracize contracted parties from participating in DNS abuse mitigation issues and ICANN in general.
	12.4. ICANN org should collate and publish	12.4. It is not clear how ICANN should implement

	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.	this recommendation. If through the ICANN Compliance process, then this will have a chilling effect on the forthright collaboration registrars and registries in the Compliance Process unless the reported data is 100% anonymized. Part of this obligation (in response to applicable laws) is outside of ICANN's remit. As this recommendation is overly broad, outside of ICANN's remit, and could reduce overall compliance, the RrSG recommends that the ICANN Board reject this recommendation.
13	**SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting** 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.	13.1. Other than spending a substantial amount of money, it is not clear what this recommendation is attempting to accomplish. There are already existing contractual obligations for accepting abuse complaints for registrars and registries, and if third parties are not able to submit abuse complaints, then they should report the noncompliance to ICANN Contractual Compliance. Any automated system has the potential for abuse - even ICANN Compliance complaints that are reviewed by a human before processing are sometimes deficient. Additionally, this proposed system will involve a number of non-contracted parties: hosting providers, registrars accredited for ccTLDs (but not gTLDs), etc. Why this should be fully funded by ICANN, and the source of this funding, is not adequately explained. As the deficiency this proposal will address has not been identified, and the average operational cost could be many multiple millions of dollars annually, the ICANN Board should reject this recommendation. 13.2. The RrSG recommends that the ICANN Board reject recommendation 13.1, so this recommendation is superfluous.
14	**SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements** 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	14.1. The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA. This

	threshold.	recommendation fails to identify the background necessitating additional requirements on registrars and registries without their participation in creating such a Temporary Specification.
	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.	14.2. The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse. If third parties have concerns or identify specific and verifiable cases of abuse, they should report them to the appropriate contracted party.
	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.	14.3. In addition to recommending that the ICANN Board reject this recommendation, the RrSG is concerned that the Review Team recommends reviewing the veracity of data leading to abuse reports (that could ultimately lead to RAA or RA termination) AFTER the reports have been sent to the contracted party. Additionally, ICANN Contractual Compliance already has a robust abuse complaint process, so it is not clear why an additional process and system is required.
	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.	14.4. The ICANN Board should completely reject this recommendation. It was created without the participation of the contracted parties, and appears to be significantly biased against contracted parties. It completely ignores the ICANN multistakeholder approach, existing ICANN Compliance processes, and it is not proper to use a Review Team to create such overbearing restrictions on contracted parties. Registrars and registrars already conduct significant amounts of anti-abuse activities, OCTO reports show that abuse is decreasing, so this recommendation appears to be vindictive rather than collaborative.
	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.	14.5. While the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed. This includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN.

15	**SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements**	
	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.	15.1. The RrSG does not support this recommendation. There is no need for an EPDP regarding abuse. The only difference between a PDP and an EPDP is that an EPDP does not have an issues report. Otherwise, and EPDP does not operate "faster" than a normal PDP[2]. As the RrSG disputes that any PDP regarding abuse is necessary (because no issues to be resolved have been clearly and articulately identified, as well as defined goals), it is imperative than any abuse PDP start with an issues report, and only then can the GNSO Council determine whether a full PDP is necessary to address the specific issues.
	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.	15.2. In addition to reiterating that the ICANN Board should reject the proposed EPDP for the reasons above, the community does not get to define how contracted parties operate. That is subject to negotiation between ICANN and the contracted parties, and limited to within ICANN remit. These proposals are outside of ICANN's remit. There are also existing structures and processes to terminate registrars and registries in the RA/RAA, no need for additional (and subjective rather than objective) methods of termination. Additionally, conducting updates every two years can be a significant community burden, and further exceeds the community's role (e.g. only ICANN and the contracted parties negotiate the contracts). Finally, making the requirements binding within 45 business days completely ignores the realities of operating a registrar or registry, and the significant resources required to make such substantial changes in a short timeline that will remove resources from supporting core business functions (e.g. provision of domain name registration services to customers).
16	**SSR2 Recommendation 16: Privacy Requirements and RDS**	
	16.1. ICANN org should provide consistent cross-references across their website to	16.1. This recommendation attempts to override an existing ICANN initiative (ITI). As the ITI has been

[2] EPDP Phases 1 and 2 did operate faster, only because of the 1-year deadline in the Temporary Specification, and the lack of continued funding for the GNSO.

	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.	in process for a number of years, and is currently focusing on high volume and high priority items, the ITI should be allowed to continue its existing timeline as the Review Team has not provided any rationale for why RDS data should be prioritized over other action items in the ITI. 16.2. The ICANN Community should not be able to dictate the composition, scope, and function of ICANN Contractual Compliance. It is an independent department within ICANN and should remain that way. Additionally "privacy requirements" are outside of ICANN Contractual Compliance's limited contractual scope. Finally, it is not the role of ICANN (or ICANN Contractual Compliance) to facilitate law enforcement needs. The RrSG recommends that the ICANN Board reject this recommendation. 16.3. Along with the rest of this recommendation, this is outside of ICANN's scope. ICANN is not a DPA, and the audit would need to cover a number of countries and jurisdictions around the world, and it is unclear how ICANN has the expertise or resources to conduct such an audit. As with many other recommendations in this Final Report, it is not clear what issue this recommendation intends to resolve.
17	**SSR2 Recommendation 17: Measuring Name Collisions** 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 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	The RrSG was not aware that name collision was a concern and thought it was previously addressed by ICANN and the community, see e.g.https://www.icann.org/en/system/files/files/ncap-study-1-report-19jun20-en.pdf.

	no financial interest in gTLD expansion.	
18	**SSR2 Recommendation 18: Informing Policy Debates** 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.	18.1. ICANN Org should determine which staff attends or participates in research, networking, and security conferences on behalf of ICANN Org, and how to report and/or share this information with the ICANN Community- not a Review Team. Utilizing this information to influence contracted party behavior is outside of ICANN's remit, and the ICANN Board should reject this recommendation. 18.2. As repeated elsewhere, contract negotiations are between contracted parties and ICANN as detailed in the RAA and RA, and are not subject to public discussion and feedback from the ICANN community, including recommendations from peer-reviewed literature. 18.3. The RrSG recommends that the ICANN Board reject this recommendation, as it is not clear how the studies will be paid for, and how confirming peer-reviewed studies are beneficial or within ICANN's remit.
19	**SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite** 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.	19.1. and 19.2 are both outside of ICANN's remit, and it is also not clear how ICANN will pay for this.
20	**SSR2 Recommendation 20: Formal Procedures for Key Rollovers** 20.1. ICANN org should establish a formal	The RrSG does not have a position on this recommendation.

	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.	
21	**SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators** 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.	The RrSG does not have a position on this recommendation.
22	**SSR2 Recommendation 22: Service Measurements** 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	The RrSG does not have a position on this recommendation.

	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.	
23	**SSR2 Recommendation 23: Algorithm Rollover** 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	The RrSG does not have a position on this recommendation.
24	**SSR2 Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process** 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.	The RrSG does not have a position on this recommendation.

Sincerely,

Ashley Heineman
RrSG Chair