Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response					
BC	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	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.	Strong support	No action required	Broad community support for Rec. 10, including GAC, BC, IPC, WIPO, FIRST; NCSG, RrSG oppose; SSAC asks for clarification	Agree	1) Clarify, update, combine Recs. 2) As a general point, the report should make clear that the independent review team does not accept a stalemate where (a) many agree that contractual provisions are not sufficiently strong but (b) no one is empowered to do anything about it. 3) Suggest we group CPH contract-related recommendations together and note multiple review teams + advisory cmts input is community input to direct ICANN Org contract negotiations. 4) Clarify who should establish the performance metrics, and that it's an operational issue not policy.				
SSAC	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	(3.3.2) Unless the underlying contractual commitments exist to compel contracted parties to act within clearly defined parameters and responsibilities, then the compliance measures proposed here seem ineffectual. Does the SSR2 RT believe that these contracts are sufficiently prescriptive with respect to behaviours and the residual issue is simply one of enforcement of compliance? As the report notes, "Compliance has few options to enforce the agreements" and the measurements proposed in this recommendation appear to 5 measure ineffectuality of enforcement. Are there measures that could have a beneficial outcome on improving this space?	Seeks clarification	Clarify text, noting where conracts can be enforced w/ clear and intentional Compliance action, and where contracts need to be improved via negotiations w/ contracted parties	See column I and add more information	Agree; clarified text					
NCSG	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	#Recommendation 10: The SSR2 team justifies, elaborates more, analyzes impact and compares what they are recommending here to the current modes of operations, We also note that the recommendation strays into suggesting board action on areas which the review team is not empowered to comment on such as current GNSO policymaking.	Clarification needed	Clarify what requires Board, staff and contracted party action and what requires PDP	See column I and add more information	Disagree, see explanation					
RrSG	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	In general, this recommendation is for policy and should go through the ICANN policy process. Regarding the sub recommendations:	Clarification needed	Clarify what requires Board, staff and c	See column I and add mo	Disagree, see explanation					
RySG	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	The RySG notes that Compliance's size and scope has grown exponentially in recent years and we disagree with SSR2's characterization and implication that contractual compliance is so under-enforced or under-resourced that entire new teams need to be hired to deal with specific issues. We note this throughout the report, but call it out specifically here.	Disagree			Disagree, see explanation					
IPC	10		The IPC is generally supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The RT recommends, and the IPC supports, several methods for ICANN to better utilize its relationships with the Registrars and Registries to combat DNS abuse, including SSR2 Recommendation 10: "Improve the Framework to Define and Measure Registrar & Registry Compliance," SSR2 Recommendation 15: "Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse," and SSR2 Recommendation 16: "Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats." The IPC supports these recommendations and any steps to more effectively combat DNS abuse relating to the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts. ... Accordingly, the IPC supports these SSR2 recommendations that would require meaningful enforcement of existing obligations of registries and registrars to prohibit certain security threats and abusive activities, enhance such requirements to further mitigate such activities, include real consequences for registrants who engage in prohibited abusive behavior, and and consistent investigation and response to reports of abuse by registrars.	Agree	Clarify per details	See column I and add more information	Agree, clarified text					
ICANN Board	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	the Board asks the SSR2 RT to clarify what functionality beyond complaint handling, audits, breach notices, suspensions, and terminations it seeks ICANN Compliance to implement within the scope of the agreements. The Board asks that the SSR2 RT provide greater details on what issues or risks exist from the current operational model, how the SSR2 RT recommendation will address them, and what relevant metrics could be applied to assess implementation. Further, it is unclear what is meant by the terms "performance metrics framework", "guide level of compliance", and "other elements that affect abuse, security, and resilience". The Board suggests that the SSR2 RT provide more detail on the intent of this recommendation to ensure that it is properly considered for implementation. The Board notes that this recommendation may overlap with recommendations from the Initial Report on New gTLD Subsequent Procedures (Section 2.12.3), the Registration Directory Service (RDS)-WHOIS2 Review Final Report and recommendations (4.1, 4.2, and 5.1), and CCT Review Team Final Report recommendations (21). The Board requests clarification on the intent of recommendation 10.1 in light of this potential overlap.	Clarification needed	Clarify per details	See column I and add mo	More details have been added; the Board (and staff) should review decades of discussions and written comments by non-contracted parties impacted by abuse and contracted party action to gain a deeper uderstanding of Compliance problems, user needs, and required improvements					
RrSG	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.	10.1 - This is already covered by ICANN- Compliance metrics on complaints, Compliance audit, Whois ARS, monitoring by GDD tech team, etc	Clarification needed	Clarify per details	See column I and add more information	Disagree, see explanation					
RySG	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.	Compliance-related recommendations must be linked to specific contract terms. "Other elements that affect abuse, security, and resilience" is too vague to be implementable. The RySG believes this is out of scope of SSR2.	Clarification needed; in scope	Clarify per details	See column I and add more information	Disagree					
RrSG	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.	10.2 - This is something Compliance already does. A review team, with limited understanding of the operation and structure, should defer to Compliance to determine how it will best allocate resources.	Disagree	Clarify per details	See column I and add more information	Disagree					
RySG	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.	The RySG does not see the value in specific compliance officers to handle specific contractual compliance issues. All of Compliance is capable of responding to compliance complaints and ICANN has demonstrated that it's capable of conducting a full audit of all Ry contracts on a specific issue, like SLAs.	Disagree	None		Disagree					
SSAC	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).	(3.3.3) Given that the report has noted some challenges relating to enforcement of agreements with contracted parties, it is unclear what the review and the subsequent "recommend the inclusion of requirements" precisely entails. Which party is to perform these reviews? Is it the team envisaged in recommendation 10.2? If not then who would be performing such a review? If so, would these compliance officers possess the skills to be able to, "recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident"? Who is to receive the review's recommendations? What criteria would be used by this party to assess these recommendations for additional requirements? If requirements are being proposed, where is the contractual foundation to enforce these requirements? Does recommendation 10.3 implicitly refer to recommendation 15, where changes to the contractual conditions are proposed? Some further clarity on these recommendations would be helpful to understand both the detail of the proposed actions and the overall intent of these recommended measures.	Clarification needed	Clarify per details	See column I	Text clarified					

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
RrSG	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).	10.3 - It is the position of the RrSG that contract negotiations do not originate from review teams or working groups. That is reserved for ICANN Org, and the RrSG/RySG.	Disagree	None	None	Disagree
RySG	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).	The RySG believes that this is outside the scope of the SSR2's work. The RySG notes that there is an established contract amendment process: consensus policy and negotiations between CPs and ICANN. This recommendation has no basis in policy or fact - it is a conclusory statement that presupposes the question. If the SSR2 has identified problems with performance metrics, then it could recommend that ICANN and the community study them. In this case, the SSR2 is proceeding down the same slippery slope as CCT-RT in recommending solutions without recommending ICANN first engage in exploration and work to determine if a solution is needed.	Disagree	None	None	Disagree
RrSG	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.	10.4 - It is not for a review team to determine the pace of the PDPs or IRTs. There can be unexected issues that arise (as during the implementation of EPDP Phase 1), and it is better for ICANN to develop and implement policy properly rather than rushing to meet an artificial deadline.	Misinterpreted SSR2 Rec	Clarify	Clarify	Misunderstood Rec.; clarified
RySG	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.	The RySG notes that this recommendation is not made to the appropriate party. A recommendation on a GNSO policy process should be referred to the GNSO Council as the manager of the policy process. Furthermore, it's outside the scope of a review team to recommend that a PDP wrap up (as it undoubtedly will even without the RT's recommendation).	Misinterpreted SSR2 Rec	Clarify	Clarify	Misunderstood Rec.; clarified
GAC	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.	The GAC also agrees with Recommendation 10.4 on implementing the EPDP policy recommendations within 1 year.	Agreed	None	None	Agree
IPC	10.4		While the IPC is supportive of the intent behind recommendation 10.4, it notes that it is not the role of the Board to direct the outcome or timing of a community-led PDP. The RT may wish to revise this language, for example to refer to the Board itself, and via Org, offering all necessary support to achieve the desired outcome	Misinterpreted SSR2 Rec	Clarify	Clarify	Misunderstood Rec; clarified
BC	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	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 asubject 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 other types of abuse) to accurately describe problems being addressed.	Agreed	confirm "consideration by the entire community" is this reflected, do we want that?	Stalemate situtation is highly problematic. No one responsible - no change. Address this concern in text.	Agree
NCSG	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	#Recommendation 11: As this related to the definition of DNS Abuse, we believe that it is highly important to elaborate more on the methodology and the validation mechanisms.	Details should be provided in the subsequent implementation plans	Check ISO and NIST	Review whether more detailed implementation guidance is appropriate	Agree that ICANN Org implementation plans should provide details on methodology and validation
RrSG	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	The RrSG has concerns about this recommendation. The ICANN community is currently engaged in abuse and threat activities, as are the contracted parties. The definition of abuse and threats can be difficult to define broadly, which is perhaps indicitive why there is not a definition that satisfies the review team. It is essential that contracted parties, which have undertanding of implications of these activities, be involved in the process (rather than the ICANN board engaging only security-related community members).	Never said RrSG shouldn't be involved as part of community	Clarify community involvement	Clarify	Misunderstood Rec.; as w/ all groups, RrSG should be involved; however, this effort should not be driven by CPH's (or ICANN Org's) desire to minimize their responsibilities, accountability or cost.
GAC	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	The GAC welcomes Recommendation 11 on efforts to implement current community vetted definitions of DNS Abuse without delay and the need to ensure that definitions evolve to meet continuing threats, in the context of efforts aimed at finding a more effective approach to address DNS Abuse, including with the GAC's support through its advice, comments, and correspondence. Although the GAC shares the overall goal of achieving clarity and consistency with regard to the definition of DNS Abuse and Security Threats, it is not quite clear how the different processes suggested in Recommendations 11.1, 11.3 and 11.4 should interrelate. The GAC therefore invites the Review Team to consider, in view of existing procedures and rules, how this goal can be best achieved.		Check relations 11.1, 11.3, 11.4 -- how does this make sense. Tighten up wording and be explicit. Add text on what process could look like.	Clarify, add more detail	Agree; clarification and more detail provided
IPC	11		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. As a preliminary matter, the IPC supports SSR2 Recommendation 11: "Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions" and any related efforts to define abuse so that reporting and consequences for abuse can flow more efficiently from an agreed-upon definition.		None		Agree
RySG	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.	The RySG does not think it is feasible or realistic for there to be "universally acceptable agreement" on definitions for abuse, SSR, and security threats but is willing to continue its extensive ongoing discussions to try to reach such an agreement.	Disagree that a feasible and realistic abuse definition can't be achieved and evolved for ICANN purposes.	Clarify explanation.		Disagree with contention that such an abuse definition is not feasible.
SSAC	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	(3.3.4) If the underlying issue is that SSR2 has found evidence that the ICANN Board and ICANN org are not properly processing and acting on the outcomes of other reviews then it should say so explicitly. This recommendation that refers to recommendations from other reviews tends to suggest such a conclusion without actually saying so.	Clarify explanation of underlying issue	This is clearly an issue: whois/rds, atrt, ssr1, etc. not our issue to solve but state facts.	Clarify	Agree. Clarified.
ICANN Board	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	The language of this recommendation presupposes that each of the recommendations are (1) accepted or approved by the ICANN Board; and (2) prioritized by the ICANN community for immediate implementation. The Board notes that it does not believe this to be within scope of the SSR2, and is not aligned with the Bylaws. Additionally, the Board seeks clarification regarding whether this recommendation makes sense in terms of resource deployment in light of the ongoing community discussions regarding the definition of "DNS abuse". The Board also seeks clarification of the information the SSR2 RT has to support its position that the definition of abuse has been vetted through the bottom-up multistakeholder process.	Clarify explanation	Clarify in explanation. Footnote "vetted definition". Not in scope: strategic plan. Clarify community vetted. Number / specify ssr related recommendation, clarify that those are in scope.	Clarify	Disagree with Board's/Staff's interpretation and understanding. Team has documented how it's in scope, why it should be prioritized, and we've shown where ICANN's own records show definitiion vetting. Logic requires multiple things to interact.
RySG	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	The RySG is unclear about what the SSR2 is asking given Recommendation 1 is to implement the remainder of SSR1 recommendations. We do not support the Board unilaterally adopting the definitions established by either the SSR2, the CCT-RT, or the RDS/WHOIS2 Review without full community adoption.	We're not suggesting "unilaterally adopting definiitions established by" review teams.	Clarify	Clarify	RySG seems to have misunderstood Rec. Clarified.

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response					
SSAC	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 Communique 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.	(3.3.5) What specific actions did the SSR2 RT have in mind? It is challenging to understand the intended objectives of this particular recommendation given the imprecision of the term "encourage community attention".	Clarify. Provide more detail but not too much detail as to trigger Staff objection that it's too detailed and prescriptive	Clarify	Clarify	Clarified.					
ICANN Board	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 Communique 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.	In reviewing recommendations 11.2 and 11.3 together, the Board requests clarification as to the intent of these recommendations and whether the SSR2 RT believes it prudent to "implement the SSR-relevant commitments (along with CCT and RDS recommendations) based on current, community vetted abuse definitions, without delay", knowing that the definition may/will evolve. Furthermore, the Board seeks clarification as to how the SSR2 RT would assess effective implementation of this recommendation. It is not clear what the measure of success would be given that the Board cannot mandate the community to reach agreement on the definition of "DNS abuse". It is also not clear what the SSR2 RT intends for the Board to do in "adopting" a definition. The Board believes that the issue is not about "abuse definition", but about what kind of DNS abuse is within ICANN's remit.	See actions >	Re-commit to action on current defition, update it regularly (because abuse is not static). Rewrite to achieve smart goal. What abuse is in ICANN's remit. Clarify what ICANN cannot handle would actually help.	Clarify	Clarified.					
RySG	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 Communique 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.	The RySG believes this work is ongoing but objects to the conclusion of this Recommendation as to which definition the Board should adopt. If 11.3 is to be included as a recommendation, the RySG would only support the text "ICANN Board should encourage community attention to evolving the DNS abuse definition".	While it's clear RySG would prefer a never ending conversation about abuse definition rather than abuse mitigation actions and accountability measures, that's not what SSR2 is recommending or what is needed to support internet SSR.	That is true. Action is needed now plus community attn to evolving definition. Need to clairfy to specify how to get there and then have it adopted.	Clarify	Clarified.					
SSAC	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	(3.3.6) It appears that the part of this recommendation that refers to SSAC actions is already underway with the formation of a DNS Abuse Work Party within SSAC. SSAC would be happy to brief the SSR2 RT on the objectives of this DNS Abuse Work Party. The SSR2 RT should consider whether to retain Recommendation 11.4 or simply note in the report that this activity is underway within SSAC.	SSAC action alone will not achieve objective, especially with contracted parties active role in "Abuse Work Party," and SSAC's non-transparent, closed efforts. This is why PSWG needs a leading role and CPH involvement shouldn't be controlling this effort.	Schedule a talk with the group.	Clarify. These two comments are going into different directions. Comments show that community seems divided on this. Crime is government business, maybe others can chime in but gov is the party that needs to act.	Clarified.					
RySG	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	The RySG believes this is a policy matter and outside the scope of SSR reviews - if the Board would like the community to try to define DNS abuse, then it can instruct the community to do so, but it's inappropriate to recommend that the definition come solely from two ACs (SSAC and GAC) without input from the rest of the community.		This is a public safety issue. Remove attack surface: what we meant is to def have experts involved. Roll into 11.3.?							
BC	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	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.	Noted. Suggest they start with action on Crossroads report on registrar violations. Suggested approach need to be discussed in Team meeting.	include examples in text	Clarify	Clarified					
NCSG	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	#Recommendation 12: This recommendation is outside of the review team remit and is already addressed by current ICANN Policymaking in the GNSO and thus should be removed.	Disagree. Among other things, It's an SSR1 Rec. which, in addition to impact on SSR, puts this in the team's remit.	WHOIS is clearly SSR, should be stated. Might want to mention that this is EPDP material.	Clarify	Disagree. Among other things, It's an SSR1 Rec. which, in addition to WHOIS documented impact on SSR, puts this in the team's remit. Clarified					
WIPO	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	ICANN's continued delay in facilitating a centrally-coordinated mechanism for standardized access to non-public registrant data is harming a range of legitimate causes, including law enforcement, security researchers, and intellectual property owners and consumers.1 Beyond fostering scalability and predictability in all stakeholders' interests, developing such an access model would remove a current risk faced by Contracted Parties in assessing WHOIS disclosure requests.2	Noted and could be merged with risk and compliance while noting the remit.	Note	Agree. Note	Agree.					
RySG	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	The RySG does not support SSR2 making this recommendation given the ongoing EPDP Phase 2 work and questions how this falls within the scope of this review.	Disagree. Among other things, It's an SSR1 Rec. which, in addition to impact on SSR, puts this in the team's remit.	WHOIS = SSR, ack epdp	Disagree. Clarify	Among other things, It's an SSR1 Rec. which, in addition to WHOIS documented impact on SSR, puts this in the team's remit. Clarified					
IPC	12		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." Recommendation 12 addressing WHOIS data addresses issues raised by many in the community including the Security and Stability Advisory Committee (SSAC), Governmental Advisory Committee (GAC), BC, and IPC. It is important to the issue of addressing abuse that registrant data is correct, and available through the proper channels or to the proper authorities.	Noted and could be merged with risk and compliance while noting the remit.	None	Agree. No action needed	Noted and the issue addressed has been streamlined with other related recommendations.					
SSAC	12.1	The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement.	(3.3.7) The SSAC largely agrees with the intent of this recommendation, while noting that this measure admits the risk of unintended consequences when considering the generality of the Internet and the diversity of bodies that enforce national regulations. How could ICANN minimize such risks in the context of the implementation of this recommendation?... This general recommendation appears not to take into account the existing activities in this area.		Address consequences, confirm activities.		Noted and more specific language included in recommnedations.					
RrSG	12.1	The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement.	Regarding recommendation 12.1, this is currently being addressed by EPDP Phase 2, and should not be subject to another PDP.	Noted but not in agreement for its removal given the steps being taken for the EPDP and need for consensus. There can be a refernce to the process as a noting and re-emphasise SSR2 team belief that this issue be specifically addressed.(https://www.icann.org/public-comments/epdp-phase-2-initial-2020-02-07-en)	Word this as SSR inpout to this issue.		Noted and more specific language included in recommnedations.					
RrSG	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.	For recommendation 12.2, as indicated previously, there is a pending IRT that is dealing with complex issues. The IRT should be allowed to proceed at its current pace to ensure quality outcome (rather than rushing to meet an artificial deadline).	Noted. Suggested approach need to be discussed in Team meeting.			Noted and more specific language included in recommnedations.					
BC	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	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.	BC agrees	no action needed		Agreed					
M3AAWG	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	(5) We recommend that the SSR2 make clear that rate limiting is an impediment to the DAAR system's ability to accurately report registrar statistics.	Accept	Mention rate limiting for anti abuse and also researchers. How can this be solved? Give to the board to sort? Include in contratct updates	Add to report	Agreed. Added	*				

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
SSAC	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	(3.3.8) It is unclear if "completeness" here refers to the limited realm of second level domain names in gTLDs. If the intent is a far broader scope of "completeness" including all top-level domains (TLDs) and all labels to an arbitrary depth of delegation, then it would be helpful if the report indicated how such an extension of this activity could take place. Also, the draft report should clearly indicate what is actionable with the specific recommendations, and more precisely, how effectiveness can be measured. Who should get the Domain Abuse Activity Reporting (DAAR) reports, and what should be made public, needs further attention in this recommendation. The SSAC suggests that further consultation within the ICANN community on DAAR methodologies would be helpful.	Want further clarification, what's actionable, how to measure effectiveness. who should get reports. SSAC should have done this already, but I guess it falls to SSR2 to do the work	Clarify. Add details	Clarify. Add details	Noted; more details added. SSR2 also recommends that SSAC bring more attention and guidance to this.
WIPO	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	To the extent ICANN would consider UDRP cases as part of any DAAR or Domain Name Marketplace Indicators, it should be noted that while the UDRP supports consumer trust, this is trust earned only after significant time and expense is invested by brand owners (and in some cases only after a fraud has been perpetrated on end users). The continued availability of the UDRP, as operated by WIPO on a not-for-profit basis, moreover benefits Contracted Parties and ICANN by keeping them out of disputes. **The fact that WIPO has seen record-breaking numbers of UDRP cases over the years illustrates that the root issue of cybersquatting is not itself being addressed.** To this end ICANN may wish to look at programs instituted in the .EU and .DK domain spaces.	Ask WIPO for more infol	Ask WIPO for more info	Unclear yet	Noted. **action pending
ICANN Org	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	Work is already underway by ICANN org towards implementation of this recommendation. If the SSR2 RT's intent is to recommend implementation of something beyond what is in progress with ongoing work, ICANN org encourages the SSR2 RT to provide specific details.	(kc has clarification from ICANN Org on exactly what is underway and how they are measuring its effectiveness.) Clearly ICANN has not met its own objectives of "develop [ing] a robust, reliable, reproducible, and replicable methodology for analyzing security threat activity that can then be later used by the ICANN community to facilitate informed policy decisions." DAAR falls far short of this goal in practice and lacks sufficient information to be able to tel, for example, which registrars or registries are harboring significant abuse, which kinds, etc.	TBD	Clarify (kc input needed)	Clarified
IPC	13		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." ... As for the DAAR, the IPC commends ICANN's intended goal of "develop[ing] a robust, reliable, reproducible, and replicable methodology for analyzing security threat activity that can then be later used by the ICANN community to facilitate informed policy decisions." However, the RT's assessment finds that the DAAR falls far short of this goal in practice because it lacks sufficient information to be able to tell which registrars or registries are harboring significant abuse. The IPC supports the RT's recommendation to include this critical data and turn the DAAR into a powerful tool for accountability and transparency in the domain name registration system. ... The IPC does however note that a number of brand owners now operate Brand TLDs under Specification 13, in which, due to the nature of these TLDs, the risk of DNS abuse is low. In making recommendations that seek to impose additional obligations for monitoring and reporting, the IPC would urge the RT to acknowledge differing risk profiles and avoid imposing unnecessary and costly burdens on Brand TLDs. In particular, this might include different requirements for access to Brand TLD zone files through the CZDS, different security threat monitoring and reporting requirements, and different audit approaches with respect to maintaining the security of a Brand TLD.	agrees	recommend avoid imposing unnecessary and costly burdens on Brand TLDs. In particular, this might include different requirements for access to Brand TLD zone files through the CZDS, different security threat monitoring and reporting requirements, and different audit approaches with respect to maintaining the security of a Brand TLD.	Clarify	Agreed. Clarified.
RrSG	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.	Regarding recommendation 13.1, this data is already being published elsewhere. It is outside of ICANN's scope to aggregate and republish this data. It is also not clear that DAAR is incomplete or ineffective, so additional information is needed to know how the cost for these additional resources outweighs any benefit.	Aggregating and republishing data IS within ICANN's scope; see IPC, BC comments as one of many explanations of how DAAR is incomplete and ineffective.	cite actual documentation that daar is incomplete/ineffective. explain how cost outweighs benefit. explain R&Rs will inherently resist accountability for abuse.	Add more explanation.	Disagree. Aggregating and republishing data IS within ICANN's scope. See IPC, BC comments, among others, for input on how DAAR falls short, is incomplete and ineffective. More information added.
ICANN Org	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.	ICANN org solicits input from all stakeholders on how to improve DAAR on a regular basis, including via daar@icann.org and the "DNS abuse measurements" mailing list	Based on publicly available comments, ICANN Org has repeatedly failed to follow thru on DAAR-related requests. Soliciting input is not the same thing as working with entities fighting abuse to improve DAAR. this mailing list doesn't have any traffic right?	Reinforce action and outreach in terms hopefully ICANN staff will understand.	Add more explanation.	Disagree. Available information indicates a lack of outreach outside the ICANN community, and a lack of follow-through on input from non-contracted parties whowant to improve both measurement and reporting of domain abuse.
RySG	13.1		The RySG notes that the ONLY entities that can take down domain name abuse are: registries, registrars, hosts, and registrants. There are no third parties that mitigate abuse: only third party tools that analyze data and report on that data.	Abuse take downs are a separte issue from measurement and reporting of abuse	Check explanation to see if further calrification is needed.	< see	Abuse take downs are a separte issue from measurement and reporting of abuse; we'll seek to clarify
ICANN Org	13.2	ICANN Board should annually solicit and publish feedback from entities inside and outside the ICANN community that are mitigating abuse in order to help enhance ICANN org's data on domain abuse activity.	This appears to be duplicative of 13.1. ICANN org encourages the SSR2 RT to clarify the differences in these two recommendations.	Merge, remove duplication	merge 13.1,13.2	< see	Clarified
BC	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	While the BC historically has discouraged ICANN Org from engaging on matters of pricing, thisdata could be informative and helpful in identifying and targeting sources of DNS abuse. The BC supports.	Agrees w/ Team	no action	no action	Agreed
SSAC	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	(3.3.9) Given that ICANN has deliberately distanced itself from any role as a regulator of pricing in this space and holds a position where market forces determine pricing, then what is the context of this analysis and how could such a rigorous quantitative analysis inform the mechanisms of market-based pricing? Further elaboration of the envisaged use of such an analysis would be useful to understand the intended effect of this recommendation. If this recommendation is an oblique reference to heavily discounted prices being applied to bulk name registration practices, then is the underlying abuse issue pricing or bulk registration?	Collecting and analyzing data related to price is completely separate from "regulation" or ICANN being a "regulator" and there has been no suggestion relating to "market-based pricing." Enough questions have been raised about the relationship between registration payments and abuse to warrant quantitative analysis. The "use" is factual information and a more comprehensive understanding of DNS abuse.	Clarify. further elaorate intended effect.	Clarify	Collecting and analyzing data related to price is completely separate from "regulation" or ICANN being a "regulator" and there has been no suggestion relating to "market-based pricing." Enough questions have been raised about the relationship between registration payments and abuse to warrant quantitative analysis. The "use" is factual information and a more comprehensive understanding of DNS abuse.
RrSG	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	The RrSG notes that this was already recommended by CCT. The ICANN board deferred implementing and stated "questions raised regarding the value of the data" (see https://www.icann.org/en/system/files/files/resolutions-final-cct-recs-scorecard-01mar19-en.pdf). It is not clear what will be accomplished by collecting this information. There are extensive reports already that tie low cost, or free registrations to abuse activity (which are havens for abusive domains, along with low cost hosting). Additionally, ICANN is likely not in a position to determine a full picture due to the large and varying promotional pricing, or prices set by resellers of registrars, or for registrars that do not provide this information publicly. This could be a massive undertaking which might not produce useful information.	See above	See above	Disagree; Clarify	See above. There's value in this data for those studying and fighting abuse across sectors. As a steward for the DNS this falls squarely in ICANN's remit and should be done by experienced, external researchers.

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
WIPO	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	Part of any meaningful look at payments for domains used to perpetuate abuse would also look at data accuracy under the umbrella of anti-fraud know-your-customer norms (which would in turn call for a timely resolution of PPSAI independent of EPDP work).	Good point. Should add privacy/proxy implementation (PPSAI) to Rec 12 on WHOIS EPDP	< see	Acknowledge, add to Rec 12	Agreed
RySG	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	The RySG does not support this recommendation as it is out of SSR2's remit. The RySG notes that ICANN is not a price regulator and is unclear what benefit would come from this research. Further, the RySG is concerned that this recommendation presupposes a relationship between the price of domain names and evidence of "security threats and abuse". The RySG refers to its previous comments on collecting pricing data made in response to the CCT-RT Final Report, particularly recommendations 2, 3, and 4.	It's clearly within SSSR2's remit. See above comments regarding the difference between analysis and regulation, and benefits of research. The "registration experts" -- RrSG says "There are extensive reports already that tie low cost, or free registrations to abuse activity (which are havens for abusive domains .."	@@heather can you go get those previous comments? i think we should include in report.	Disagree, clarify	Disagree & clarify. per above
IPC	14		The IPC is supportive of this recommendation.		no action needed	No action	Agreed
ICANN Board	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	The Board notes that this recommendation seems to raise similar questions the Board noted when considering recommendations from the CCT Review Team about collecting pricing data (see page 4 of the scorecard with regard to CCT recommendations 3 and 4). With regard to the relevant CCT Review Team recommendations, the Board placed them in "Pending" status, and directed ICANN org, through engagement of a third party, to conduct an analysis to identify what types of data would be relevant in examining the potential impacts on competition and, whether that data is available, and how it could be collected in order to benefit the work of future CCT Review Teams. The Board stated that this analysis would inform the Board's decision on next steps and whether the recommendations could be adopted. Given this background, the Board would like to understand whether the SSR2 RT has considered the Board's previous concerns and how that has been factored into its deliberations.	Enough statements and questions have been raised about the relationship between registration payments and abuse (Also see RrSG comments, above) to warrant quantitative analysis. The "use" is factual information and a more comprehensive understanding of DNS abuse. It has been nearly two years since the CCT Review final report was submitted with a related recommendation and there has been no reported follow-up, which indicates that this needs to be reinforced as an SSR priority and given the attention and action it deserves by the Board and ICANN Org.	Provide more explanation. Address board concerns by explaining our position.	More explanation.	It is, in part, becasue of the work and recommendations of the CCT Review team, and the Board's lack of follow through that reinforced our inclusin of this recommendation. We hope the Board will take this recommendation more seriously this time and act on it. As noted above, this needs to be reinforced as an SSR priority and given the attention and action it deserves by the Board and ICANN Org.
IPC	14.1		While the IPC is strongly supportive of the intent behind recommendation 14.1, it notes that new gTLD registries are not under a contractual obligation to disclose their wholesale pricing and that efforts to gather this information from registries voluntarily during previous reviews (such as CCT) and PDPs (such as RPMs) have been unsuccessful. The RT is encouraged to revisit and refine this recommendation, for example to encourage Org to seek to include obligations during contract renewal/contract negotiations to disclose pricing information on a confidential basis for the use by RTs and PDPs and/or for Org to consider whether registrar retail pricing can meaningfully inform this issue.	Agree that this should also be considered but note that ICANN Org, in the last negotiation over changes to the base new gTLD registry agreement, deleted a requirement for Registries to share pricing data with ICANN.	Change text to incorporate.	Agree. Add text	Agreed; incorporated
BC	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	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 to non-public Whois data, with vigorous enforcement of that access right given to ICANN as a compliance matter 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.	no action needed	none	none	Agreed; incorporated
M3AAWG	15	In its review of ICANN org's activities, the SSR2 RT found that the publications, statements, and related actions by ICANN org 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.	(intro) We concur with the SSR2 RT assertion that "the publications, statements, and related actions by the 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". The report should further urge the ICANN organization to be transparent and to exercise its ability "to negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission" (See ICANN Bylaws, Article 1, Mission at https://www.icann.org/resources/pages/governance/bylaws-en/#article1).	agreed; negotiations recommendation included above; and see note below	Use that cite. Clarify per below	add cite	Agreed; incorporated
M3AAWG	15		(3) We recommend that the SSR2 RT urge ICANN to adopt a contract negotiation process in which the influence of contracted parties who pay fees to ICANN cannot be held in question.	Agreed	Clarify -- ICANN should use process where community provides input, data on stuff that matters, consultation should be more regular, some documentation should be provided, compare CISO comment.	Clarify	Agreed; incorporated
M3AAWG	15		(4) We urge the SSR2 RT to recommend that contracted parties be obligated by contract to accommodate the high-volume needs of operational security users. Mechanisms such as whitelisting, vetting or pre-authorization which unfairly encumber academics, individuals who responsibly investigate abuse, and generally any party who has legitimate purposes to collect registration data, should not be used.	Agreed	Incorporate. Vetting and whitelisting with logging	Add	Agreed; incorporated
SSAC	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	(3.3.10) This appears to be a more detailed and clearer restatement of Recommendation 10.3, and in this light Recommendation 10.3 appears to be somewhat unnecessary.	Merging Recs	Merge recs.	Marging Recs	Agreed; incorporated
RrSG	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	It is the position of the RrSG that contract negotiations should originate through ICANN, the RrSG, and the RySG, rather than a review team. Any recommendations for changes to the RAA or RA are out of scope.	Disagree and the Bylaw mandate of this review places this matter within SSR2's scope.	Review team can recommend to board to include guidance and objectives in negotiations and processes to improve community input into negotiations, transparency of negotiations, and outcomes that serve the public interests (not to be confused with the interests of Registrars, Registries, or ICANN Org)	None	Team has recommended actions (that are within our Bylaws-mandate and scope) to improve SSR and serve the public interest.
WIPO	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	ICANN could consider incentives such as "audit credits" to incentivize adoption of best practices.	Discuss	Discuss	?	Consdering
RySG	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	The SSR RT has no authority to make recommendations to enhance or make changes to the Registry or the Registrar Accreditation Agreements and strongly objects to this set of recommendations. Similarly, the ICANN Board has no authority to implement the recommendation/s. The RySG opposes this recommendation because it presupposes the outcome of work that should be done by the community and, in several places, seems to try to preempt (and end-run around) work being done in the community and by other PDPs, such as the EPDP. Furthermore this recommendation is wholly outside the scope of the SSR2's remit (e.g. setting threshold to trigger "automatic" contract defaults). Perhaps the scope of SSR3 will be to review the outcome of the various work in progress today, but this RT is not tasked with using the Recommendations of the RT to hammer home viewpoints on how the Board and the community should presume to resolve ongoing work.	Review team can recommend to board to include guidance and objectives in negotiations and processes to improve community input into negotiations, transparency of negotiations, and outcomes that serve the public interests (not to be confused with the interests of Registrars, Registries, or ICANN Org)	Clarify this is future-looking, no unil. ateral changes.	Clarify	Disagree. The review team gives recommendations to the board on how to approach future contract negotiations. Team has recommended actions (that are within our Bylaws-mandate and scope) to improve SSR and serve the public interest.
IPC	15		The IPC is generally supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The RT recommends, and the IPC supports, several methods for ICANN to better utilize its relationships with the Registrars and Registries to combat DNS abuse, including SSR2 Recommendation 10: "Improve the Framework to Define and Measure Registrar & Registry Compliance," SSR2 Recommendation 15: "Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse," and SSR2 Recommendation 16: "Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats." The IPC supports these recommendations and any steps to more effectively combat DNS abuse relating to the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts. ... Accordingly, the IPC supports these SSR2 recommendations that would require meaningful enforcement of existing obligations of registries and registrars to prohibit certain security threats and abusive activities, enhance such requirements to further mitigate such activities, include real consequences for registrants who engage in prohibited abusive behavior, and motivate active and consistent investigation and response to reports of abuse by registrars.	Unclear, discuss (seems IPC is agreeing with Team's recommendations so no action needed?)	None?	None?	Agreed; incorporated?

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
ICANN Board	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	As noted with regard to SSR2 recommendation 11.2, the Board seeks clarification regarding whether this recommendation would be reasonable in terms of resource deployment in light of the ongoing community discussions regarding the definition of "DNS abuse". Further, as noted above, the Board cannot unilaterally impose new obligations on contracted parties through acceptance of a recommendation from the SSR2 RT. The Registry Agreement and Registrar Accreditation Agreement (RAA) can be modified either via a consensus policy development process or as a result of voluntary contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome.	Evolving the definition of "DNS Abuse" is an ongoing responsibility, not an excuse for inaction. See above for the role the Board should play, along with ICANN Org, in serving SSR needs and the public interest, when negotiating Registrar and Registry agreements. While the Board cannot "ensure a particular outcome" in these negotiations, it can demonstrate interest and leadership in this impactful undertaking that has been ignored for too long.	Further explanation. The board can instruct negotiators to include these consitions, we note PDP might be needed.	Further explanation	Board responsibility and recommended action clarified.
ICANN Org	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.	ICANN org notes it is unable to unilaterally "make SSR requirements mandatory...". Neither ICANN org nor the Board can unilaterally impose new obligations on contracted parties. The Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board). ... ICANN org therefore encourages the SSR2 RT to consider the ongoing community discussions regarding the definition of "DNS abuse" and how to measure "DNS abuse" through metrics and reporting in finalizing this recommendation, as noted by the Board.	Evolving the definition of "DNS Abuse" is an ongoing responsibility, not an excuse for inaction. See above for the role the Board should play, along with ICANN Org, in serving SSR needs and the public interest, when negotiating Registrar and Registry agreements. While the Board cannot "ensure a particular outcome" in these negotiations, it can demonstrate interest and leadership in this impactful undertaking that has been ignored for too long.	Discussions have taken place for years, impact is low. We recommend to board to instruct negotriators, and to initiate relevant PDO		Board and ICANN Org responsibility and recommended action clarified.
RrSG	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	For recommendation 15.4, the RrSG supports the use of the GNSO to develop ICANN policy.	Considering that the registrars and registries control the GNSO Council and PDP outcomes, one would expect such support, which raises questions about the efficacy of ICANN's processes and the Team's recommendation.	None	None	Agreed but a more balanced GNSO and PDP process is needed.
BC	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	The BC applauds this common sense recommendation and encourages ICANN Org and the Board to institute incentive policies as a matter of priority.	no action needed	no action needed	no action needed	Agreed
M3AAWG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	(7) Make all forms of pricing, including promotional pricing and bulk registration pricing, a matter of public record and "open data". We concur with the SSR2 RT recommendation that ICANN should study pricing, yet urge the review team to further ask that registries and registrars share pricing with ICANN as a matter of contract, and that ICANN publish pricing at its web site, in machine usable formats.	Agree, but would note that staff deleted what little price reporting requirements there were in the new gTLD base registry agreement.	Include pricing more clearly	Add text	Agreed; incorporated
M3AAWG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	(8) We urge the SSR2 team to call for further economic modeling and study of the DNS economy by qualified professionals instead of explicit pricing recommendations.	Discuss	third party, external review? discuss	unclear?	?
SSAC	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	(3.3.11) The SSAC notes that this recommendation may be premature, as it presupposes the results from the activity proposed in Recommendation 14. The SSAC has some concerns regarding the propriety and practicality of this recommendation. This proposal may transfer abuse behaviour into those parts of the domain name space that are not directly subject to the same incentives and constraints. Such a program may be extremely difficult to manage and its effectiveness difficult to measure. This recommendation also proposes a shift of ICANN's role, as ICANN has moved away from a price regulatory role and towards an environment where pricing is a function of market dynamics. ...	Need to change "pricing" to "fees"; SSAC is conflating separate ideas.	Clarify	Clarify	Recommendation clarified
RrSG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	While this recommendation appears to be a good start, it must be subject to a PDP to determine if incentives are a good mechanism to address security threats. As for incentives, they are usually subject to abuse itself and or gaming (and bad actors will figure out a way around it).	ICANN Org's record of unilaterally using fee reductions to incentivize Registrar actions (and ICANN Org's unilateral changes in Rgy fees) indicates that the RrSG is incorrect. RrSG and RySG should provide input on the incentive process to help prevent gaiming.	Clarify and advise their involvement to improve implementation. We acknowledge that gaming incentives is an issue; while it will happen, process should increase "water level".	clarify	Clarified
ICANN Org	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	ICANN org notes that neither it nor the Board can unilaterally impose new obligations on contracted parties. The RA and RAA can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board). Further, ICANN org encourages the SSR2 RT to consider and describe what the likely externalities of incentivizing certain behavior might be so that the ICANN org and Board may comprehensively assess the impacts of the implementation of this recommendation.	Wow. Staff should know this. See above. Provide citations.	This incorrect: note that PIR has one and is effective.	Add citation	Disagree. Additional information provided.
RySG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	Again, the RySG opposes this recommendation because it's outside the scope of the RT's role.	See review team's bylaw mandate, which places this SSR-driven recommendation in scope.	none	none	Disagree; see Bylaws mandate
IPC	16		The IPC is generally supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The RT recommends, and the IPC supports, several methods for ICANN to better utilize its relationships with the Registrars and Registries to combat DNS abuse, including SSR2 Recommendation 10: "Improve the Framework to Define and Measure Registrar & Registry Compliance," SSR2 Recommendation 15: "Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse," and SSR2 Recommendation 16: "Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats." The IPC supports these recommendations and any steps to more effectively combat DNS abuse relating to the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts. ... Accordingly, the IPC supports these SSR2 recommendations that would require meaningful enforcement of existing obligations of registries and registrars to prohibit certain security threats and abusive activities, enhance such requirements to further mitigate such activities, include real consequences for registrants who engage in prohibited abusive behavior, and motivate active and consistent investigation and response to reports of abuse by registrars.	none	none	none	Agreed
ICANN Org	16.1	SSR2 Recommendation 16.1: "commercial providers"	Requests for clarification of terms	Add footnote defining commercial providers	add footnote	add footnote	Footnote added
ICANN Org	16.1	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).	As noted in the section "Requests for Clarification of Terms," ICANN seeks clarification regarding the term "commercial providers". ICANN org also notes that this recommendation may overlap with ongoing work related to the Competition, Consumer Trust, and Consumer Choice Review Team (CCT RT) recommendations. The Board passed through CCT recommendation 12 regarding incentives to the New gTLD Subsequent Procedures PDP Working Group (see page 2 of the scorecard). ICANN org encourages the SSR2 RT to consider the ongoing work of the New gTLD Subsequent Procedures PDP Working Group with regard to applicant fees and whether this recommendation may overlap with that work.	Review team is aware of the Board and ICANN Org's actions and inactions) on CCT Review recommendations, as well as the New gTLD Subsequent Procedures PDP working group's activities and their limited utility for improving SSR and mitigating abuse.	none	Add footnote on PIR's success with this approach with registrars it does business with.	The activity noted was taken into account by the Review Team. This recommendation should be adopted and implemented to improve SSR and help mitigate abuse.

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
RrSG	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.	Recommendation 16.2 is outside of ICANN's remit, and the source of funding for this is not clear (e.g. what would ICANN cancel to pay for this).	This is clearly within SSR2's Bylaw mandate. Perhaps the several million ICANN is receiving from Verisign could help cover the cost without canceling antying? Funding decisions rest with the Board.	None	None	Disagree. It is within SSR2's mandate and funding decisions rest with the Board.
ICANN Org	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.	ICANN notes that both in Recommendation 15.4 and 16.2, the SSR2 RT recommends that ICANN org "institutionalize training and certifications." ICANN org requests clarification regarding the SSR2 RT's expectations for training and certifications (i.e., types, methods) as well as the intended meaning of "institutionalize." Is the SSR2 RT requesting that general training courses be offered, for example through ICANN Learn, regarding SSR-related topics such as abuse? ... Is the intent of the SSR2 RT's recommendation to go beyond such activities? Is the SSR2 RT recommending that a more formal certification program be created, where, upon completion, parties are "ICANN-certified" in SSR-related issue mitigation? It is not clear who the intended audience of the training and certification is as the SSR2 RT mentions several parties. Would training and certification be offered to any interested party? Depending on the SSR2 RT's expectations, ICANN org has concerns with the feasibility of implementing such global certification programs. Finally, if the SSR2 RT is referring to more stringent requirements to complete training or certification, such as potential obligations in contracts, this is not within ICANN org's remit to unilaterally impose, as such changes could only come about via consensus policy development or voluntary contract negotiations (as noted by the Board).	Clarify relevant parties, registries and registrars, plus ICANN.	Clarify	Clarify	Clarified
BC	17	Establish a Central Abuse Report Portal	The BC concurs with this recommendation.	ok	None	None	Agreed
RrSG	17	Establish a Central Abuse Report Portal	It is not clear what are the "relevant parties" in this recommendation. If only registrars and registries, then such a system will likely cost more than any perceived benefit. If it is intended that it would be all inclusive (e.g. P/P providers, hosting providers, etc), it would be outside of ICANN's scope.	Clarify relevant parties, registries and registrars, plus ICANN.	Clarify	Clarify	Clarified
WIPO	17	Establish a Central Abuse Report Portal	In addition to a Central Abuse Report Portal, any measures that ICANN or a Contracted Party implements to address a reported abuse should be published along with the responses.	A categorical reponse might be appropriate	Add?	Add?	Agreed; added??
RySG	17	Establish a Central Abuse Report Portal	The Registry Agreement requires an email abuse point of contact (POC) on a per-registry basis. Any change to this requirement needs to be the result of a PDP or contract amendment. The RySG further reiterates its concern with the use of the "abuse" terminology in this recommendation. The RySG is also unsure why the responses must be publicly searchable, especially considering that they may contain confidential, sensitive or personal information, and that the disclosure of such information could disrupt in-process law enforcement investigations or violate the privacy rights of data subjects.	There could be a delay to making data available. Data should be anonymized and presented in categories. Abuse emails should not disappear. System implementation might even be based on email if CC prefer.	Clarify	Clarify	Clarified
IPC	17		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." Recommendation 12 addressing WHOIS data addresses issues raised by many in the community including the Security and Stability Advisory Committee (SSAC), Governmental Advisory Committee (GAC), BC, and IPC. It is important to the issue of addressing abuse that registrant data is correct, and available through the proper channels or to the proper authorities.	ok	None	None	Agreed
SSAC	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.	(3.3.12) The SSAC suggests that this recommendation be given a clearer rationale and also should note that any implementation of such a measure should carefully mitigate the inherent risks of undertaking this role of intermediary in abuse reporting.	Rationale: ease of use, tracking of enforcement action, identification of problem parties.	Clarify	Clarify	Clarfied
ICANN Org	17.1	SSR2 Recommendation 17.1: "abuse report"	Requests for clarification of terms				
ICANN Org	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 notes that there are no details or rationale for this recommendation in the "ICANN Compliance" section of the SSR2 draft report. It is difficult for ICANN org to determine how the review team envisions the operational details and measures of success for this recommendation. For this reason, ICANN org encourages the SSR2 RT to clarify the identified issues or risks that led to this draft recommendation, how the recommended solution will address these issues or risks, the expected impact of implementation, or what relevant metrics could be applied to assess implementation.	Abuse reports are not working right now, emails often fail to create impact. Portal increases ease of use and simplifies ensuring that reports are correctly formatted and complete to allow for action. This will cut down on time being wasted on reports that are incomplete or go to the wrong party. Overall, this will provide better security and anti-abuse action, without costing CP more money.	Clarify	Clarify	Clarified
BC	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	The BC concurs with this recommendation. 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 musthave an effective, accountable compliance function; further, to ensure activities are effective, ICANN's contracts with registries and registrars must be in order and enforceableby compliance	OK	none	none	Agreed
SSAC	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	(3.3.13) The SSAC is unsure of how this recommendation materially differs from Recommendations 10 and 15.	Recommendations merged	Recs merged	Recs merged	Recommendations merged, clarified
WIPO	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	To support the recommendation of ICANN increasing its Compliance efforts, serious considerationshould be given to addressing – to use ICANN's word – the "discrepancy" identified in ICANN's letter of February 12, 2020 to the Business Constituency that ICANN's compliance obligations are limited to ensuring that a registrar includes an abuse policy clause in its registration agreement. Such self-imposed limitation can hardly be said to underpin a compliance program that is stated to support the security and stability of the global Internet, upon which business and consumers rely.	Fair point	Address	Address	Agreed; clarified
RySG	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	The RySG is unclear why this recommendation is being made. Although SSR2 flags that the contractual obligations are implemented differently by each contracted party, the RySG notes that the contracts do not prescribe uniform or required mechanisms for contracted parties to meet their obligations. There is presently no SLA that can be pointed to in order to determine, unequivocally, that a contracted party is "aiding and abetting systemic abuse," nor does it make sense to try to measure contracted party behavior in this way. This recommendation should be reconsidered.	Add additional explanation	Clarify	Clarify	Clarified

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
IPC	18		The IPC is supportive of this recommendation.	OK	none	none	Agreed
RrSG	18.1	ICANN org should have compliance activities audited externally and hold them to a high standard.	Regarding recommendation 18.1, the RrSG supports that ICANN Compliance should be subject to outside audit.	OK	none	none	Agreed
ICANN Org	18.1	ICANN org should have compliance activities audited externally and hold them to a high standard.	ICANN org encourages the SSR2 RT to clarify the identified issues or risks, how the recommended solution will address them, the expected impact of implementation, and what relevant metrics could be applied to assess implementation. Particularly, ICANN org seeks clarification on the following: ● Who does the SSR2 RT envision conducting the external audit? ● What would the criteria be for an external audit and how would the criteria be applied? ● What is a "high" standard? Who determines that and how is it measured? Further, ICANN org notes that the RDS-WHOIS2 Review Team reviewed ICANN Contractual Compliance activities (see RDS-WHOIS2 Review Final Report) and made a number of recommendations. The Board took action on the RDS-WHOIS2 recommendations in February 2020 (see RDS-WHOIS2 Recommendations, CC.3 - approved, R4.1 and R4.2 - placed in pending status).	Many of these issues should be addressed by ICANN Org in a proposed implementation plan	Clarify	Clarify	Clarified
M3AAWG	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.	(2) Empower ICANN Compliance with contracts and enforcement tools to mitigate domain abuse.	OK	none	none	Agreed
RrSG	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.	For recommendation 18.2, the RrSG notes that these obligations exist in the RAA and Compliance already monitors it.	They misunderstand the recommendation if they think it is already being done.	Is clarification needed? Or is their statement disingenuous?	?	?
ICANN Org	18.2	SSR2 Recommendation 18.2: "as defined by the SLA"	Requests for clarification of terms				
ICANN Org	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.	ICANN org notes the ICANN Contractual Compliance team does react to complaints and enforces the contractual obligations in the RA and the RAA. ICANN org seeks clarification on what the SSR2 RT means by "systemic abuse," and the definition used by the SSR2 RT, as well as the meaning of "aiding and abetting" in the context of the recommendation provided by the SSR2 RT. ICANN org would also request clarification regarding which SLA the SSR2 RT is referring to, and why the SSR2 RT feels that this SLA is appropriate in this context.	Clarify	clarify	clarify	Clarified
RrSG	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 recommendation 18.3, ICANN Compliance already does this (see https://features.icann.org/compliance/dashboard/report-list).	Clarify	clarify	clarify	Clarfied
ICANN Org	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.	ICANN Contractual Compliance strives to have clear and efficient processes and keep those who make complaints informed and satisfied. If SSR2 RT has data indicating Compliance has not met those goals, ICANN org encourages the SSR2 RT to present the data and develop recommendations that clearly identify ways in which it believes Compliance can better perform their functions to address the deficiencies documented in that data. It is unclear what SLAs SSR2 RT is referring to and with whom those service level agreements would be made. With regards to "maximum public disclosure," ICANN org suggests it would be helpful for the SSR2 RT to document what information should be disclosed, particularly in light of GDPR-related privacy requirements, to whom, and by what means?	ICANN Org should review the decade of input from groups representing complainents, such as the BC and IPC, which does not support a claim that ICANN Compliance has "clear and efficient processes and keep those who make complaints informed and satisfied." Clarify SLA	clarify SLA	clarify SLA	Clarified
BC	19	Update Handling of Abusive Naming	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.	ok	none	none	Agreed
SSAC	19	Update Handling of Abusive Naming	(3.3.14) The rationale that reducing the potential for name similarity contributes to improved security of the DNS can be countered by the desire to express names meaningful to humans in the DNS in the languages, scripts and glyphs that humans use. There is a tension here between utility and security that the report does not cover in sufficient depth. SSAC notes that Recommendations 19's consideration to 'update handling of abusive naming' may be an inappropriate designation of responsibility. ... These recommendations would benefit from an assessment of what falls under ICANN org's remit to enforce, and what efforts ICANN org may be able to facilitate to support a broader community of interest.	The recommendation does not recommend deleting names, we should clarify that we are calling for more oversight and checks, not "censorship".	Clarify	clarify	Clarified
WIPO	19	Update Handling of Abusive Naming	Using so-called homograph spoofing, cybersquatters sometimes take advantage of visual similarity between character sets. ICANN may wish to explore technical (if not contractual) means to enforce the prohibition on the registration of mixed-script domain names combining ASCII with non-ASCII characters which do not minimize user confusion.	This is something we should consider. Might have to have carve outs for places that use both (e.g. a firm might on purpose use latin + cyrillic for all their stuff)	?	?	?
RySG	19	Update Handling of Abusive Naming	The RySG believes that this recommendation is outside the scope of SSR2 and does not support it.	Might be correct, should consider how to tackle that.			
IPC	19		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." ... The IPC also strongly supports and commends the RT's Recommendation 19 to target abusive naming in the DNS. Cybercriminals are assisted in their attacks on individuals and companies through use of misleading names, oftentimes channeling a trusted or well-known name (including in many cases a trademark), to gain the trust of their victims. The IPC encourages ICANN to adopt this recommendation and take steps to make it more difficult for a cybercriminal to take advantage of abusively misleading names.	ok	none	none	Agreed

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
RrSG	19.1	ICANN org should build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable	Recommendation 19.1 is something that is already shared among commercial and community-driven threat exchanges and are used by many companies for their endpoint protection. It is not for ICANN to aggregate and provide these services for free (as some of them are available for purchase)	Just because someone makes money off it?	Clarify ICANN role?	Clarify?	Clarified?
ICANN Org	19.1	SSR2 Recommendation 19.1: "misleading naming"	Requests for clarification of terms	Names that could mislead reasonable person potentially by accident. SAS example.	Clarify	Clarify	Clarified
RrSG	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.	Recommendation 19.2 is not clear. If a misleading domain names become abusive, then it will be listed in the feeds DAAR uses automatically.	Yes, but not as separate category.	Clarify	Clarify	Clarified
ICANN Org	19.2	SSR2 Recommendation 19.2: "misleading naming" and "abusive naming"	Requests for clarification of terms	see above, latter is to mislead on purpose.	Clarify	Clarify	Clarified
ICANN Org	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.	Without clear definitions of "misleading" and/or "abusive", it is difficult to identify bestpractices for mitigation and establish criteria that distinguishes between the two. ICANN org notes ongoing discussions related to the definition of "DNS abuse". However, we are unaware of any consensus within the community on the definition of "misleading". Beyond this, ICANN org notes that in order for an abuse type to be included in DAAR, ICANN org needs a public reputation feed that meets the documented OCTO curation criteria1. ICANN org encourages the SSR2 RT to suggest such a feed for what it considers "misleading" and "abusive" naming to be. Further, ICANN org cannot unilaterally develop policy. ICANN org suggests that the SSR2 RT consider directing this element of the recommendation to the Generic Names Supporting Organization (GNSO) Council for review as to whether the recommendation should be considered in a consensus policy development process. See also the ICANN Board comment pertaining to draft recommendations outside of the Board's oversight responsibilities.	misleading is a word used in normal language, it is pretty clear.	Clarify	Clarify	Clarified
IPC	19.2		The IPC understand the DAAR to be a collection of existing, publicly available feeds. The IPC suggests that this recommendation might better be expressed as "ICANN Org should seek to identify and incorporate feed(s) tracking this type of abuse in the DAAR. We would also encourage ICANN org to include information covering cybersquatting within the meaning of "abusive naming" for purposes of reporting and other requirements around anti-abuse measures, to the extent this category is not already explicitly covered.	Discussion required	?	?	?
RrSG	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.	For recommendation 19.3, such data needs to be curated and require a Traffic Light Protocol for sharing such information. Furthermore, this requires a clear definition of what is misleading and what can lead to abuse.	Add this in? Makes some sense.	?	?	?
RrSG	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.	Recommendation 19.4 should originate from a PDP rather than a review team. Additionally, it is not the place of a review team to initiate RAA or RA negotiation or changes.	A PDP was not required to create, implement and update the Guidelines so it stands to reason that this recommendation wouldn't require a PDP to apply to contracted parties either https://community.icann.org/display/IDN/IDN+Implementation+Guidelines	none	none	Disagree; a PDP was not required to create, implement and update the Guidelines so it stands to reason that this recommendation wouldn't require a PDP to apply to contracted parties
RySG	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.	The ICANN IDN Guidelines should not duplicate, potentially putting itself in conflict with the Registry Agreement or ICANN policies, what otherwise can be applied in a more general way to all types of domain names, ASCII and IDN. For example, Specification 7 (Rights Protection Mechanisms) of the 2017 Base Registry Agreement applies equally to all domain name registration regardless of the script used. Further, there seems to be the incorrect perception that ICANN does not enforce the IDN Implementation Guidelines upon gTLD registries, when the opposite is true. ICANN uses the Registry System Testing process to evaluate registry operator's implementation of the IETF Standards and IDN Guidelines (i.e. Specification 6 of the 2017 Base Registry Agreement), prior to delegation and when required by a new Registry Service Evaluation Process. If the registry operator does not meet the requirement as set forth in their registry agreement, then the registry operator needs to remediate the issues before ICANN approves any registry service.	We need to collect evindence on this.	?	?	?
IPC	19.4		The IPC encourages the RT to expand on this recommendation, which presently lacks clarity and specificity. The recommendation might include specific reference to cybersquatting and the use of IDN homoglyphs to mimic trademarks as an example of abusive naming through IDNs.	Correct, incorporate.	?	?	?
ICANN Board	1, 2, 5, 6, 7, 8, 9, 10.1 and 29.		The Board's draft proposal for resourcing and prioritization of community recommendations developed with input from leadership of all specific review teams, notes that an effective recommendation should address an observed issue that has significant consequences for ICANN as a whole. Clear articulation of the observed issue gives insight into the intent of the recommendation and the justification for why it should be adopted. With this in mind, the Board notes that a number of the SSR2 RT's recommendations, as currently drafted, do not clearly define the identified issues or risks, the rationale for the recommended solutions, the expected impact of implementation, or what relevant metrics could be applied to assess implementation. Some examples as outlined in this comment include SSR2 RT recommendations 1, 2, 5, 6, 7, 8, 9, 10.1 and 29.	Clarify	Clarify	Clarify	Clarified
ICANN Org	1, 2, 5, 6, 7, 8, 9, 15.3.4, 15.3.5, 18, 19.1, 19.2, 23.1, 26.2, and 29.2		ICANN org reiterates the Board's comment that it is helpful for the ICANN org, Board, and community to have an understanding of the particular issues or risks that each recommendation intends to address. A number of SSR2 recommendations, as currently drafted, do not clearly define the identified issues or risks, how the recommended solution will address the issues or risks, the expected impact of implementation, or what relevant metrics could be applied to assess implementation (for example, SSR2 recommendations 1, 2, 5, 6, 7, 8, 9, 15.3.4, 15.3.5, 18, 19.1, 19.2, 23.1, 26.2, and 29.2). ICANN org encourages the SSR2 RT to clarify these elements of each recommendation for the Board to properly consider the recommendations and make appropriate instructions to the ICANN org and/or community.	"	"	"	Clarified
ICANN Board	1.1, 12, 15, 18.2, 19, and 29, and 22.1		The Board notes that a number of the SSR2 RT's recommendations currently directed to the Board are outside of the Board's oversight responsibilities. For example, the Board cannot unilaterally impose new obligations on contracted parties through acceptance of a recommendation from the SSR2 RT. The Registry Agreement and Registrar Accreditation Agreement (RAA) can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome. The Board suggests that the SSR2 RT consider directing these recommendations either to ICANN org for inclusion in a future round of voluntary contract negotiations and/or to the GNSO Council for review as to whether the recommendation should be considered in a consensus policy development process. Some examples of recommendations to which these observations apply include SSR2 RT recommendations 11.1, 12, 15, 18.2, 19, and 29. Further, the Board suggests that the SSR2 RT consider directing SSR2 RT recommendation 22.1 to the Root Server System Governance Working Group which has recently been formed.	It is the Board's responsibility to adopt or reject a review team's recommendations The review team's recommendations are submitted to the Board and if a recommendation requires an SO, AC or ICANN Org action, it is the Board's responsibility to refer that recommendation to the appropriate party for action, track it, and ensure appropriate resolution. There is ample history of the Board's responsibility and action on review recommendations (https://www.icann.org/resources/reviews/specific-reviews) where the Board accepted recommendations, directed the CEO to proceed with their implementation, and for recommendations involving an ICANN group, the Board requested that group's action and coordinated activities between the Board and that group to oversee implementation. Further, in the past where review recommendations involved a policy development effort, the Board directed preparation of an Issue Report as part of a Board-initiated GNSO policy development process. The review team disagrees with the new approach the Board has taken since the IANA transition and the removal of the US Department of Commerce's oversight, and urges the Board to once again embrace its accountability and review commitments, and reassert its leadership responsibility on these critical reviews.	add explanation	add explanation	Disagree; added clarifying text
RySG	10, 11, 12, 13, 14, 15, 16		Finally, and critically, the RySG does not support the conclusions SSR2 has reached on the next steps, in particular, recommendations for unilateral contract amendments, or pre-determined outcomes of studies or policy work, as we believe both are outside the scope of SSR2's work. Reviews, while an important part of ICANN's accountability mechanisms, cannot be used to circumvent the policy development process, such as by attempting to impose new contractual obligations on contracted parties. The RySG would also ask SSR2 to refrain from making recommendations which refer to, or overlap with, existing recommendations from other reviews such as RDS-WHOIS 2, CCT-RT, Registration Data EPDP Phase 2, NCAP and potential recommendations from ATRT3.	They have mis-stated the facts and intentions of the team's recommendations	clarify	clarify	Disagree; the team has made recommendations in line with its Bylaw mandate and has done our best to further clarify recommndations

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
i2Coalition	10, 12, 15, 16		However, the recommendations overreach this remit, in terms of ICANN's governance and functioning mechanisms, as they advocate in a number of recommendations for unilateral, top-down action from the Board or ICANN Org on new and/or under-development policy matters. Specifically, recommendation 10 (Improve the Framework to Define and Measure Registrar & Registry Compliance) which is rated with a High Importance, and has among its sub-recommendations unilaterally amending contract clauses (10.3) and closing the EPDP while unilaterally implementing a new WHOIS policy (10.4). Further, recommendation 12 outright describes the direct and sole role that the Board should play in the creation of legal and appropriate access mechanisms to WHOIS data. Even more, recommendations 15 and 16 argue for "enhancing" and "changing" contracts, respectively. All three recommendations, 12, 15 and 16 are rated High Importance. We ask that the draft report be revised to take these concerns into consideration. We believe that the topics of resilience, security, and stability are crucial, and they should be taken seriously by those in charge of reviewing them for the ICANN ecosystem. Arguing for unilateral changes to contracts and getting ahead of the Policy Development Processes are not and cannot be normal recommendations to come out of such a review.	They have mis-stated the facts and intentions of the team's recommendations	clarify	clarify	Disagree; the team has made recommendations in line with its Bylaw mandate and has done our best to further clarify recommndations
FIRST	10,11,13		FIRST therefore welcomes the SSR2 recommendations 10, 11 and 13 and looks forward to seeing an implementation of these recommendations.	ok	none	none	Agreed
RySG	10.1, 11.2, 15.1,		the RySG encourages the SSR2-RT to spend some additional time considering what it hopes to achieve by reiterating CCT-RT recommendations, and reconsider whether they are truly necessary within an otherwise very robust set of recommendations. The RySG considers the implementation and completion of outstanding SSR1 recommendations as the key priority. In particular, the RySG believes that the remit of SSR needs to be clearly defined so that it can properly inform the scope of SSR2's work and can provide the Board with some guidance on the new recommendations.	We hope to underscore their importance and encourage Board adoption as they support SSR objectives	none	none	SSR2 has fully considered each recommendation and stands by its utility in improving SSR
GAC	10.3, 15.1, 15.2, 15.4, 16		The GAC invites the Review Team to consider the articulation between various Recommendations and to clarify how, for example, Recommendations 10.3, 15.1, 15.2, 15.4 and 16, which all propose changes to the contractual framework between ICANN and its Contracted Parties, should work together and be taken forward.	Agreed	clarify; merge	clarify; merge	Agreed; clarified and merged recommendations
GAC	10.3, 15.1, 15.2, 16		The GAC welcomes proposals for specific mechanisms as set out in Recommendations 10.3, 15.1, 15.2 and 16 to incentivize a comprehensive and effective response to DNS Abuse. The GAC has historically taken a strong interest in Registry and Registrar contractual compliance enforcement concerning WHOIS obligations, as well as other elements that affect abuse and security (See e.g., GAC Hyderabad and Copenhagen Communiqués3). Furthermore, the GAC has held regular exchanges with the ICANN Compliance Team, in writing and at its plenary meetings, in an effort to strengthen compliance mechanisms.	OK	none	none	Agreed
RySG	11, 14, 15 and 16		We would appreciate additional information from the SSR2-RT about how it reached the decision to effectively duplicate the recommendations from a previous Review Team.	Clarify the SSR utility of recommendations and encouragement of Board action	clarify	clarify	Clarified
RySG	11, 14, 15, 16		The RySG is also concerned with some of the definitions set out by SSR2 in Appendix A, in particular the definitions of "security threat" and "DNS abuse", and note that we do not support the definitions provided. Given SSR2 recommends policy work by the ICANN community to define "DNS abuse" and "security threats," the RySG would ask SSR2 to refrain from creating its own definitions. The RySG appreciates that it is useful for the SSR2 to have a working glossary to assist its work, but the working glossary should not be used to interpret the recommendations made by SSR2, or adopted as community definitions by the Board. The report seems to repeatedly conflate the terms to broadly encompass undesirable activity related to both DNS/infrastructure abuse, security threats, and IP/content-related abuse.	Clarify use of established definitiions	clarify	clarify	Clarified
NCSG	13, 14, 15, 16, 17, 18, 19, 20		#Recommendation 13 to 20: They are all related to DNS Abuse and the DNS operations and are "high" priorities. We recommend that the Review Team proposes a dedicated team, like a cross community Working Group to work on it. We believe that this represents a stronger way/metric to assess the effectiveness of the implementation of those recommendations by a future SSR Team rather than making specific recommendations at this point. We do not fully support the recommendations relating to the opening of DAAR data to private firms for their internal abuse department. This is outside of the role of ICANN and we do not support recommendations related to this topic. On abusive naming we reject the call to replicate the existing systems that were the result of GNSO policy making with regards to trademark confusion and string similarity, again we do not believe that this is within the mandate of the SSR2 RT.	Disagree; within scope	none	none	Disagree; within SSR scope
GAC	13, 19		we also welcome Recommendations 13 and 19, which encourage the collection of data on mitigating abuse to improve Domain Abuse Activity Reporting (DAAR) in order to improve both measurement and reporting of domain abuse. Most importantly, the GAC supports the suggestion that ICANN org should publish DAAR reports identifying Registries and Registrars whose domains most contribute to abuse according to the DAAR methodology.	OK	none	none	Agree
BC	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.	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.	Agreed	clarify	clarify	Agreed; clarify
RrSG	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.	Regarding recommendation 13.1.1, commercial entities already publish such data. Some of these reports include flawed, incomplete, or false positive information, so it is should not form the basis for ICANN to "name and shame" contracted parties. There are existing compliance activities to address registrars or registries that may not be complying with the RAA or RA. The recommendation does not mention the benefits and or possible issues such publication could create. This recommendation should be subject to community consideration before further action.	Disagree; and all recommendations are subject to public comment	none	none	Disagree; and all recommendations are subject to public comment
ICANN Org	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.	ICANN org is in discussions with relevant stakeholders as to how best to provide data to inform policy discussions.	ICANN Org has had several years of input and intermittent discussion without demonstrable change.	none	none	ICANN Org has had several years of input and intermittent discussions without demonstrable change. Iterative action is needed
RySG	13.1.1		The RySG notes that any RO can be the target of abusive activity (through no fault of the RO) and that publishing a list of victims is unlikely to curb actual abuse. We suggest instead focusing on understanding how various RO business models either (or both) prevent or mitigate abuse. DAAR data, without context, is just uncorroborated raw numbers. For instance, a particular RO may experience a 2% abuse rate as a daily average, however that number says nothing about how fast yesterday's domains were taken down and if the domains on today's list were also on yesterday's list.	OK	none	none	We suggest RySG provide additional information to accompany the recommended DAAR data, if they feel it's useful.
RrSG	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.	For recommendation 13.1.2, it is not clear what source data DAAR entails, and whether the sources have been vetted by contracted parties and the broader ICANN community. The recommendation is not very clear what source data for DAAR entails. This data is likely published elsewhere, and it is not ICANN's remit to provide a clearinghouse for information that can be obtained elsewhere.	Disagree	none	none	Disagree.
ICANN Org	13.1.2	SSR2 Recommendation 13.1.2: "source data"	Requests for clarification of terms	add footnote	add footnote	add footnore	Clarified
ICANN Org	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.	Publishable DAAR-related data is already slated to be included in the Open Data Platform.	"publishable" is a term ICANN Org applies too narrowly and results in publishing of DAAR data that is not actionable or enlightening.	none	none	"publishable data" is a term ICANN Org applies too narrowly and results in the publishing of DAAR data that is not actionable or enlightening and falls considerably short of what non-contracted entities requested.
RySG	13.1.2, 13.1.3		Most of the entities that collect and report on behaviors labeled "abuse" by DAAR, do so for a specific, often commercial, purpose. This data is not freely available to the world and ICANN has repeatedly explained that the contracts with the feed providers do not allow them to make the data public. We recognize that many in the community want to see this data for free and, indeed, so do many ROs. However, simply listing it as a Recommendation will not make it so.		none	none	Disagree
RrSG	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.	If recommendation 13.1.3 is referencing DAAR, then again, these feeds are already available.	nope	none	none	Disagree
ICANN Org	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.	With the inclusion of DAAR data into the Open Data Platform, this recommendation will be implemented	nope	clarify	clarify	Disagree; clarified

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response
ICANN Org	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 advisory activities that would enhance domain name abuse prevention and mitigation	It is unclear what sort of assistance the SSR2 RT is recommending; ICANN org asks the SSR2 RT to clarify this point. ICANN's Office of the Chief Technology Officer (OCTO) is particularly interested in ensuring people understand what DAAR data says (and doesn't say). Clarification from the SSR2 RT would be helpful.	clarify	clarify	clarify	Clarified
RySG	13.1.4		ICANN org has provided a tool and information. It's the community's job to determine if that information should inspire future work.		none	none	Agree, but ICANN Org has an important role to play in informing the community about abuse so policy and other activities are based on an understanding of abuse and SSR matters
RySG	15, 16		The RySG is concerned about a number of the recommendations that direct the Board or ICANN org to make changes to the Registry Agreement and note that it is not possible for the Board or ICANN org to unilaterally impose new contractual conditions on Contracted Parties. Amendments to the registry agreement are only possible via a formal amendment process or the adoption of consensus policies. We would therefore encourage the Review Team to reconsider the recommendations that direct the Board or ICANN org to make changes to the registry agreement as we do not believe they can be implemented.	addressed above	none	none	Misundertood recommendations
ICANN Org	15, 16, 19.2, 5, 6, 18, 20		ICANN org also welcomes this opportunity to provide feedback on the operational feasibility of implementation of the SSR2 RT recommendations. This comment addresses a number of recommendations that, as currently drafted, may not be feasible for ICANN org to implement because the recommendation would appear to require ICANN org to act outside of its mission and scope (for example, SSR2 recommendations 15, 16, 19.2), or the expected impact of implementation is not clearly defined (for example, SSR2 recommendations 5, 6, 18, 20). ICANN org encourages the SSR2 RT to further engage with ICANN org subject matter experts to ensure feasibility and usefulness of its recommendations.	the team welcomes additional, specific suggestions on clarifying and strengthening recommendations from ICANN Org, if they have them	none	none	the team welcomes additional, specific suggestions on clarifying and strengthening recommendations from ICANN Org, if they have them
GAC	15, 17, 29, 31		Finally, the GAC welcomes the fact that several recommendations dovetail with priorities the GAC has endorsed for its Public Safety Working Group, such as the inclusion of ccTLDs in DNS Abuse mitigation efforts and the investigation of the security implications of DNS encryption technologies (Recommendations 15, 17, 29 and 31). The GAC invites the Review Team to consider how the work of the PSWG and other parts of the ICANN community could contribute to these efforts.	not sure what else to do...	none	none	Agreed; will look for those opportunities
RrSG	15.3.1	Ensure access to registration data for parties with legitimate purposes via contractual obligations and with rigorous compliance mechanisms.	For recommendation 15.3.1, this is most likely not possible because it would violate fundamental rights of data subjects. Furthermore, the correlation between registration data and the effectiveness of actual threat mitigation is unknown.	clarify	clarify	clarify	Disagree; clarified
RrSG	15.3.2	Establish and enforce uniform Centralized Zone Data Service requirements to ensure continuous access for SSR research purposes.	Regarding recommendation 15.3.2, such research is already possible under many data protection laws. However, current ICANN community processes do not comply with these laws, and as such, the RrSG recommends that the ICANN community focus on how research in a manner that complies with existing laws (rather than making proposals that might violate those laws). The RrSG notes that ICANN OCTO has mentioned several times it does not need access to registrant data for research purposes.	OCTO is wrong	none	none	Disagree
IPC	15.3.2		The IPC would point out that many brand owners who operate Brand TLDs under Spec 13 are reluctant to have their future branding decisions telegraphed by means of the public access to the CZDS. The Brand TLDs would encourage a more nuanced treatment of CZDS access which recognizes the particular nature of a TLD.	OK	none	none	Suggest Brand TLDs engage community on this issue
IPC	15.3.3, 15.3.4		The IPC is supportive of the intent behind these recommendations but notes that ICANN has no control over ccTLDs and the ccNSO. The RT is encouraged to revisit and refine this to acknowledge this lack of control. We seek clarification as to the changes to registrant information proposed by 15.4: what changes specifically are proposed?	Report makes ccTLD involvement voluntary	none	none	Report indicates ccTLD involvement is voluntary
ICANN Org	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.	ICANN org notes that this recommendation does not include justification as to why ICANN and others would need a vetting process and encourages the SSR2 RT to provide this in its final report. Further, it is not clear to ICANN org which entities the SSR2 RT intends to be vetted or how that vetting can be implemented. With regard to the request in this recommendation to "immediately instantiate a requirement", ICANN org notes that neither it nor the Board can unilaterally impose new obligations on contracted parties. The RA and RAA can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board).	clarify	clarify	clarify	Clarified
MarkMonitor	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).	MarkMonitor supports a reduction in domain fees for retaining an agreed low percentage of abusive domain names in a registrar portfolio. We believe that in the continuous fight to prevent DNS abuse and reduce "bad actors", the positive reward for good practices should be a welcomed initiative to encourage registrars to take a proactive approach in the monitoring and enforcement actions in relation to DNS Abuse. MarkMonitor supports this novel approach to incentivise rather than chastise. In order to ensure that this is implemented successfully, we need clear definitions of the percentages to identify eligibility and also the identification method should also be defined and explained alongside the reduced fees and/ or discount.	OK	none	none	Agreed
RrSG	16.1.1, 16.1.3	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). 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.	For recommendation 16.1.1 and 16.1.3, how will ICANN offset the discount (which will result in a lower revenue for ICANN)?	Verisign's multi-million dollar gift to ICANN	none	none	SSR2 is not responsible for budget allocations
MarkMonitor	16.1.2	Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.	MarkMonitor also supports this recommendation. As with 16.1.1 the success of this initiative will be with the clear and express definition of "verified", the mechanisms that are relevant for the verification process and what the thresholds are relating to maximum submissions. This shall require more consultation with contracted parties and the review team shall need to ensure that this is implemented effectively.	OK	none	none	Agreed
RrSG	16.1.2	Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.	Recommendation 16.1.2 will be difficult to implement in light of privacy laws. There are also questions, such as how can registrars verify registrants, what will prevent bad registrars from faking the verification, and does verification mean lower abuse?	Should be addressed in ICANN Org's implementation plan	none	none	Disagreed; should be addressed in implementation plan
ICANN Org	16.1.2	SSR2 Recommendation 16.1.2: "verified registrant"	Requests for clarification of terms	add footnote	clarify	add footnote	clarify
ICANN Org	16.1.2	Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.	As noted in the section "Requests for Clarification of Terms," ICANN org seeks clarification of the term "verified registrant". Is the SSR2 RT referring to potential activities to "verify" the identity of a registrant? If this is the case, ICANN org encourages the SSR2 RT to consider this recommendation in light of ongoing discussions and work related to the European General Data Protection Regulation (GDPR), including the feasibility of conducting such activities in light of GDPR, and the impact on ICANN contracts. Specifically, depending on what the SSR2 RT means by "verified registrant", conducting verification activities could have potential implications for ongoing discussions related to access to non-public registration data as well as controllership. That is, who does the SSR2 RT envision would be conducting the verification and managing the data related to verified registrants? Additionally, ICANN org encourages the SSR2 RT to consider the potential budgetary implications of a fee reduction.	Verification of registrants is successfully done by numerous registries and some registrars. Other issues should be addressed in implementation plan.	none	none	Clarfied; severa issues raised should be addressed in implementation plan
MarkMonitor	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.	MarkMonitor supports this offering and appreciates the approach of ensuring that there is an incentive for the registry in addition to registrars.	ok	none	none	Agreed

Source	Rec	Title	Comment	Preparer Comments	Actions	General Actions	Response					
ICANN Org	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.	ICANN org notes that there are no fees for submitting Registry Services Evaluation Policy requests (RSEPs). Fees only apply if ICANN org identifies potential security or stability concerns and utilizes a Registry Services Technical Evaluation Panel (RSTEP). Is the SSR2 RT referring to RSTEP fees in this recommendation? Further, ICANN org notes concerns regarding the feasibility of implementing this recommendation as pre-approval may not be possible. ICANN org encourages the SSR2 RT to consider in its final recommendation if the Fast Track RSEP Process could be utilized to meet the intended outcome of this recommendation.	clarify	clarify	clarify	Clarfiied					
MarkMonitor	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).	MarkMonitor supports this recommendation, however we are aware that the implementation of this scheme may require considerable effort from a policy perspective. As this specific recommendation shall require clear parameters, especially the provision of what is an "appropriate" period. As per our comments and feedback, specificity is vital in the successful implementation of these initiatives and this scheme is exactly in the same vein. Also clarifying the mechanisms of how we shall identify the domain names, what constitutes a valid "take down" and what is "appropriate" will severely minimise the scope for this DNS Abuse initiative being abused itself. This shall require the most consultation from contracting parties. Ultimately MarkMonitor supports rewarding actions by contracted parties to address new forms of abuse.	Agreed; should be addressed in implementation plan; "white hat" registrars like Mark Monitor, among others, should be involved in development of plan	none	none	Agreed; should be addressed in implementation plan					
RrSG	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).	It is not clear how recommendation 16.1.4 can be tracked. As with other parts of this recommendation, it is subject to gaming/abuse. It could also lead to a new version of frontrunning (e.g. register a domain, track traffic for 25 days, then suspend for "abuse" to get money back if the domain is not generating sufficient parking page revenue or a malicious campaign ends).	Agreed; see above	none	none	Benefit outweigh risks; should be addressed in implementation plan					
ICANN Org	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).	ICANN org repeats its comments above with regard to SSR2 Recommendation 15.1, namely that consideration should be given to the ongoing community discussions regarding the definition of "DNS abuse" as well as metrics/reporting for abuse. Additionally, ICANN org has concerns with regard to how this recommendation could be effectively implemented and encourages the SSR2 RT to consider potential issues with gaming and mis-aligned incentives. For example, contracted parties might have less incentive to guard against the creation of domains intended for misuse or might in some cases even profit from their creation if they end up being "free" of ICANN transaction fees.	See previous comments	none	none	Disagree -- evolving abuse discussions should be used as an excuse to not take action; risks should be mitigated by implementation plan					
IPC	16.1.4		The IPC does not understand what is intended by this recommendation. It would appear to create the possibility of a bad-actor registrar selling such names and then rapidly taking them down, thereby receiving payment both from the registrant and a refund from ICANN. This presumably is not the intent, so the RT may wish to clarify this recommendation.	Clarify	Clarify	Clarify	Clarified					