ICANN | GNSO

Generic Names Supporting Organization

DNS Abuse Small Team Report to GNSO Council

31 July 2025

Status of This Document

This is the Report of the DNS Abuse Small Team (ST), covering topics related to DNS Abuse mitigation. The assignment given to the ST by the GNSO Council were:

- Review 2022 Small Team Recommendations;
- Assess impact of ICANN contract amendments;
- Conduct outreach to ICANN Community;
- Analyse INFERMAL study findings;
- Identify gaps in DNS Abuse mitigation efforts.

Preamble

The objective of this Report is to document the DNS Abuse Small Team`s deliberations on the assignments named above and its key findings and Recommendations.

Table of Contents

1 Executive Summary

1.1 Introduction

In early 2025, the GNSO Council reconvened its DNS Abuse Small Team with a revised assignment form to re-examine DNS abuse mitigation in light of new developments. The previous Small Team (2021–2022) had identified enforcement gaps and issued recommendations, some of which were addressed through contractual amendments to the Base RA and RAA. Those amendments (effective since 2024) strengthened abuse mitigation obligations, and ICANN Contractual Compliance has since reported initial data on their impact. With these measures in place and new research available, the Small Team was tasked to consider new insights and discuss potential next steps on DNS Abuse. Drawing from community input, compliance data, and external studies, the team was tasked with identifying remaining gaps and assessing whether further policy development is warranted.

This report presents the Small Team's findings and recommendations to the GNSO Council based on the tasks and research done as requested in the Assignment Form.

1.2 Recommendations

In view of the below findings, the DNS Abuse Small Team recommends the following:

Recommendation 1: Initiate a comprehensive Issue Report on DNS Abuse Mitigation Gaps. The DNS Abuse Small Team recommends that the GNSO Council initiate an Issue Report to further investigate the identified DNS abuse mitigation gaps and to support informed policy action.

Rationale:
The aim/purpose of the Issue Report would be:

- To confirm a given issue is within ICANN's mission,
- To explain what the issue is, who it affects and how, what support there is to address the issue,
- To recommend whether the issue(s) is within the scope of ICANN's Mission and properly within the scope of the GNSO policy development process
- To identify when a gap/issue is better addressed in a mechanism other than a PDP.

Recommendation 2: Structure the Draft Charter around Three Priority Gaps while maintaining flexibility for broader coverage. The ST recommends that the Issue Report and Draft Charter, while adhering to Recommendation 1, focus on three gaps identified through the Small Team's review of compliance/research data, community input, and gap matrix analysis.

Rationale: The ST suggests to only narrowly charter a PDP on three gaps and complete that work expeditiously. Subsequent PDPs could then be initiated from the original Issue Report, when the initial PDP completes its work.

Recommendation 3: Prioritize the following Three Identified Gaps.

Based on data analysis, community consultation, and input from stakeholder groups, the Small Team recommends the following three gaps be prioritized for further investigation under the Issue Report:

- **Associated Domain Checks:** The CPH update during ICANN83 indicated that there is currently no contractual requirement or best practice standard requiring contracted parties to investigate domains associated with known malicious actors.
- **Limited coordination on DGA-based abuse:** The current system for responding to Domain Generation Algorithm (DGA)-based threats commonly used in botnets and malware campaigns seems to be fragmented. No single trusted platform or voluntary protocol for real-time information sharing between registries, registrars, and law enforcement means fragmentation causing delays and inconsistent responses.
- **Unrestricted API access for domain name registration for new customers:** Some studies and other community inputs indicate a possible correlation between abuse and unrestricted API-enabled domain name registrations.

Rationale: While all identified gaps listed in the gap matrix will be considered as part of the Issue Report, the Small Team recommends elevating the three prioritized gaps due to their recurrence in data sources and stakeholder input. The ST has chosen the above topics from the matrix, based on topics that seem appropriate for policy development (taking into consideration review of source data, input/priorities received by ST members and Community consultation during ICANN83), meaning:

i. important/impactful gap to solve
ii. likely to gain broad consensus
iii. ideally, the potential solution(s) seem achievable having in mind current workload and resources.

The ST further notes that all identified issues should be assessed through a balanced analysis that considers the rights and responsibilities of all stakeholders involved to ensure that any policy development appropriately reflects fairness, proportionality, and due process.

Recommendation 4: Consider additional gap priorities for subsequent next steps.

In addition to the three high-priority gaps recommended for early consideration in Recommendation 3, the ST recommends that the GNSO Council and the resulting Issue Report also give due consideration to the following set (see table in section 3) of gaps identified through the Small Team's data analysis, community consultation, and matrix review. While these issues may not have emerged as the most frequently cited, several were identified by stakeholder groups as meaningful contributors to DNS abuse and merit closer examination.

Rationale: The ST thinks that these gaps will be considered more prominently within the scope of the Issue Report to support potential subsequent PDPs as noted in Recommendation 2, or alternative mechanisms as appropriate. Capturing this broader context aims to ensure that the Issue Report not only supports near-term policy action but also serves as a foundation for ongoing, phased work on DNS abuse mitigation. Once the Final Issue Report has been finalized/published,[1] the GNSO Council and the DNS Abuse Small Team will coordinate to

[1] GNSO Operating Procedures (Issue Report Formalities - p. 68 to 70)
https://gnso.icann.org/sites/default/files/file/field-file-attach/op-procedures-19sep24-en.pdf

determine when additional work or follow-up from the Small Team is needed. This alignment aims to support continued efficiency on a topic of high importance to the ICANN Community.

2 Key Findings of the DNS Abuse Small Team

Through the below methodology and based on its assignment form, the Small Team identified several gaps in existing DNS abuse mitigation frameworks. These gaps highlight that despite recent significant improvements, issues remain in current DNS abuse mitigation efforts. The Small Team believes that many of these deficiencies lie squarely within the GNSO's policy remit and merit structured policy consideration. However, it is likely that some identified gaps might not result in Consensus Policies but could be addressed via other recommendations such as non-binding best practices as opposed to formal Consensus Policy Recommendations. Importantly, the overview of gaps is not intended to be an exhaustive checklist for policy action. Rather, it serves as a strategic tool for prioritization and further investigation.

The list of identified gaps is based on a review of multiple data sources, including ICANN Contractual Compliance reports, community feedback sessions, third-party research (such as the INFERMAL study), and input from industry efforts. The ST and various SGs have reviewed and provided feedback on each identified gap, specifically, whether it should be considered a "true" gap, whether it should be considered for policy development within the GNSO remit, or any other input that should be considered. **This input and the detailed list of gaps and clustering is included in Annex A** to this document and should be considered and incorporated into the Issue Report.

The purpose of the gap overview is to systematically capture what could be considered a gap in DNS abuse mitigation across the entire domain lifecycle (as introduced by the DNS Abuse Small Team in 2022), from registration through enforcement. While various contractual amendments, industry initiatives, and compliance actions have improved DNS abuse mitigation, these efforts are not all-encompassing. Without a structured overview, it is difficult to assess the cumulative effectiveness of these efforts or understand which areas require additional attention. The List of Gaps overview aims to ensure that input from across the ICANN community, including stakeholder groups (SGs), constituencies (Cs), and external organizations, is represented and documented. This List of Gaps aims to allow for a shared understanding of the problem and promotes alignment across diverse viewpoints. Organizing gaps by lifecycle phases and thematic clusters (e.g., enforcement, proactive measures, industry coordination) helps stakeholders see where gaps exist and what stage of the domain lifecycle they affect.

The recommendations on prioritizing specific gaps (Recommendations 3 and 4) are the result of a structured assessment conducted by the DNS Abuse Small Team. The Small Team first reviewed a variety of source materials, including contractual compliance reports, the INFERMAL study, industry white papers, and prior community input, to identify and analyse a comprehensive set of DNS abuse mitigation gaps.

Following this review, ST members consulted with their respective constituencies and stakeholder groups using the assessment criteria provided in the Rationale of Recommendation 3, meaning:

i. important/impactful gap to solve
ii. likely to gain broad consensus
iii. Ideally, the potential solution(s) seem achievable having in mind current workload and resources.

The top three issues presented in Recommendation 3 emerged with the strongest support across groups and were viewed as best meeting the assessment criteria.

At the same time, additional gaps outlined in Recommendation 4, while not as frequently prioritized, were still considered important by several stakeholders. These have been identified for additional consideration in the context of this report, to support potential follow-up work, whether through subsequent PDPs or other mechanisms.

An overview of the priority outcome can be found here in table form:

Listed Priority Gap	**Gap ID in Matrix (Annex A)**	**CPH**	**CSG[2]**	**NCSG[3]**	**GAC[4]**	**ALAC**
Associated Domain Checks	C2	X	X	X	X	X
Inefficient Coordination on DGA-Based Abuse	CC1	X		X		X
Unrestricted API Access for domain name registration	P1	X	X	X	X	X
Awareness on reporting abuse	A1					X
Broaden use of abuse data for preventive action	P11					X
Continual review and update of DNS abuse definitions	CC2		X			
Lack of standardized recourse mechanisms for registrants affected by abuse-related actions	C3			X		
Validation of registrant details	P3		X			X

[2] The CSG provided their priorities during the DNS Abuse Small Team meeting on 17 July
[3] The NCSG provided their priorities during the DNS Abuse Small Team meeting on 24 July
[4] The Governmental Advisory Committee (GAC) provided their priorities in form of GAC Advice: https://gac.icann.org/contentMigrated/icann83-prague-communique

3 Methodology

The Small Team conducted a structured analysis based on its assignment form of DNS abuse mitigation across multiple phases of the domain lifecycle.

This included:

- **Data Analysis:** The Small Team reviewed ICANN Contractual Compliance reports on DNS abuse, especially post-2024 data on the efficacy of new anti-abuse contract provisions. This provided quantitative insight into complaint volumes, response times, and enforcement outcomes under the updated agreements.
- **Research Studies:** The Small Team examined informal and community-led studies of DNS abuse. Notably, the *INFERMAL* report (Inferential Analysis of Maliciously Registered Domains) was reviewed for its findings on attacker behaviour and abuse patterns. These studies helped pinpoint which abuse vectors (e.g. bulk registrations) correlate strongly with DNS abuse. Relevant industry perspectives were also considered. The Small Team reviewed recent white papers and reports from DNS abuse experts (e.g. Net Beacon's May 2025 Whitepaper on DNS abuse policy initiatives) to ensure the Team's analysis captured externally identified issues and practical recommendations.
- **Community Input:** The Team solicited and considered input from multiple ICANN community sessions and stakeholder groups, gathered during ICANN public meeting sessions and consultations. This was instrumental in understanding perceived gaps and community priorities. For example, discussions at ICANN82 and ICANN83 highlighted continued community concern and the need for coordinated response efforts.
- **Previous work on DNS Abuse:** The Small Team also reviewed the previous work done by the DNS Abuse Small Team in 2022 and discussed if further gaps remain and if all gaps from their report were addressed.

This comprehensive approach allowed the Small Team to triangulate findings and confidently identify where current mechanisms fall short. Findings were categorized by lifecycle stage and further grouped by thematic clusters to support prioritization and future policy scoping.

Annex A – DNS Abuse Small Team Gaps Matrix

Below is the table of a non-exhaustive list of gaps in DNS abuse mitigation based on the review of key sources including ICANN Compliance updates, INFERMAL study, previous DNS Abuse Small Team report and NetBeacon White Paper. This table is intended as a working document to consolidate known issues across all areas of DNS abuse response. The Small Team reviewed and provided comments on the identified gaps, particularly where clarification or correction may be needed, and to suggest any additional gaps they believed are relevant for further consideration.

Link to the original working document.

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
0	**Preventative Measures**	**P1**	**Friction**			Unrestricted API access	NetBeacon PDP Whitepaper, Workshop on CPH Ideas for Future Work on DNS Abuse	Enables rapid, automated abuse through mass registrations by unverified users. Section 3.12 of the RAA could be improved to ensure registrars that offer an API/Reseller program have the necessary contractual means to impose	RrSG: see response to G12 • Adding contractual obligation on resellers who have access to the registrars API make sense but the implementation needs to take into account the different business models. RySG feedback : • It's important to keep in mind that while this may be a feature abused by malefactors, this is not automatically an

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
								DNS Abuse mitigation requirements on their resellers.	“unverified user” problem. This is a customer behavior problem, whether verified or not, and most likely is addressed by G1 (Associated Domain Check). • Clarification needed re usage of "verify" in gap description to mean "verify" under the RAA vs another concept of "verification"? At-Large (High Priority) -INFERMAL report indicates high correlation of API bulk registration and abuse -Unrestricted API access allows bots to register thousands of domains instantly, often for short-lived attacks. ADDITIONAL GAP: -Need for introducing friction in API access should also be expanded to

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									existing customers CSG feedback: - CSG agrees with ALAC and conclusion of INFERMAL. Bulk registration misuse outweighs potential benefits.
0	**Preventative Measures**	**P2**	**Friction**			Lack of Proactive/timely Syntactic and Operational Validation	INFERMAL	Some of the tested registrars did not fully validate registrant contact info (e.g., phone numbers are often unchecked) allowing attackers to register domains using fake or throwaway data with little friction.	RrSG • syntactic validation and contactability should be the focus rather than ""accuracy"" or ""verification"" as neither ""accuracy"" nor ""verification"" have been shown to decrease DNS Abuse in the namespaces that practice these—and every namespace that does does so in a different manner • This sounds appropriate under existing policy • that's been an obligation since the 2013 RAA

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									amendment, there is no need for a new policy." CSG feedback: - Syntactical and operational validation are hollow measures and are subject to throwaway data. No evidence suggests this is effective against abuse mitigation. - ccTLDs that more stringently validate have much lower instances of abuse, as we all know. - Registrars fully validate data to reduce fraud when it suits their business models (e.g., auctions), so there's obvious merit to the procedure.
0	**Preventative Measures**	**P3**	**Friction**			Lack of Proactive/timely verification	INFERMAL	Allows abuse using fake credentials and disposable contact info.	RrSG • Friction is one way that many Contracted Parties decrease abuse of their namespace (friction in

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						at registration			access, friction in cost, &c.) however, the type of friction implemented will differ by business model and is not something that it is reasonable to attempt to dictate across the entire industry • Additional Info: from our experience stricter verification measures only allows to catch the low hanging fruit. Criminals who register malicious domain names have access to accurate but stolen information. Furthermore, for the lazy ones, suspending for inacurate data is a great tool for registrars as it remove the burden of having to judge of the abusive nature of the domain name use. (this how we suspend ""crypto scam"", we are not equipped to judge of the

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									legimacy of a token or a marketplace. RySG feedback : • INFERMAL points out that Registrars have 15 days to complete this. If that's not being done then this seems like an ICANN Compliance issue, not a policy issue. • Clarification needed re usage of "validate" in gap description to mean validation requirements of the RAA are not being followed or if they're not sufficient; and confirming needed that "validate" is intended and not "verify" At-Large (High Priority) • Better checks, proper verification, and clear data on bulk registrations would slow down and help prevent abuse • No proactive verification

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									means abuse domains go live immediately, often harming users before any checks are done. TO NOTE: • Should move towards identity verification down the line CSG feedback: - Risk-based verification already is being recommended by governments (see NIS2 Article 28 implementation guidelines); better to get ahead of the trendline before it becomes mandatory across the board. - Agree with ALAC regarding immediacy of user harm; "register first and ask questions later" is an abuse-permissive strategy.

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
0	**Preventative Measures**	**P4**	**Friction**		INFERMAL	Lack of data on bulk registration abuse	DNS Abuse Small Team Report (2022)	Unclear which bulk registrations are malicious; legitimate and abusive uses are hard to distinguish.	RrSG: see response to G12 RySG feedback : • Comment: a data point: https://dnsrf.org/blog/bulk-registrations-uncovered--legitimate-uses-vs--cybercriminal-exploits/index.html • See also comment for item G2 above. At-Large • The lack makes it hard to separate malicious patterns from legitimate activity, limiting informed action. Hence, introducing friction at the point of registration is one of the most effective ways to prevent abuse before it reaches the end-user.
0	**Preventative Measures**	**P5**	**Proactive vs reactive**			Minimal Deterrent Effect of Reactive	INFERMAL	The study states that domain uptime (i.e., how long a malicious	RrSG • the proactive measures that most Contracted Parties undertake are

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						Measures (Uptime)		domain remains active) has little influence on attacker behavior. Even short uptimes (under an hour) can yield valuable credentials, meaning fast takedowns alone are insufficient to deter abuse.	necessarily invisible because the abuse never happens; there is no incentive to us to promote DNS Abuse: we do have a number of proactive measures to prevent fraud and reduce abuse of our namespaces • the landscape is constantly evolving and our respective fraud departments evolve with them—not only is it happening, it would be folly to attempt to chase it with Policy (see: blocking VPNs; this may help some registrars combat fraud but would disrupt other registrars' valid customers; it should not be a blanket prohibition) • Additional info: not recent but still relevant https://www.infosecurity-magazine.com/news/84-of-ph

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									ishing-sites-last-for-less/ RySG feedback : • Uptime of abuse is distinct from takedowns and these must not be coupled. No specific action is going to deter abuse, the fact that action is taken is going to deter abuse. Phishing can be mitigated without a takedown and that uptime matters here, as well as uptime related to all mitigation methods for all types of abuse, which may or may not involve a takedown.
0	**Preventative Measures**	**P6**	**Proactive vs reactive**			Challenges in real-time detection of short-lived abuse	NetBeacon Blog Analysis (2024) - Impact of ICANN Contract	Lag in DNS data allows short-lived malicious domains to evade detection.	RrSG: see response to G11

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
							Amendments		
0	**Preventative Measures**	**P7**	**Proactive vs reactive**			Underuse of predictive algorithms for early detection	DNS Abuse Small Team Report (2022)	Predictive tools could help identify patterns of abuse, but are not widely implemented.	RrSG: see response to G11 • This will only work at the registry level, registrars view is limited to their registrations, they don't know if and when criminals will start targetting them. " RySG feedback : • The idea of proactive restrictive measures seems to be overestimated, all it can do is to make a notification (RA and RAA 2013 does not allow for cancellation of registrations without a reason (something in the PAST, not in the FUTURE) At-Large (High Priority) • Reactive actions are not enough. Many attacks succeed in minutes. We

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									need tools that predict and detect early to really protect users. • There is a growing number of ccTLD using machine learning and AI to proactively identify suspected abusive domain names and subject the registrant to heightened verification. NCSG (Re: Reactive vs. Proactive Measures) - Well-implemented reactive measures can be as effective as proactive strategies in addressing abuse. - However, overly broad or premature proactive interventions (e.g., preemptive takedowns, automated flagging) can generate false positives, unjust suspensions, and chilling effects on lawful

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									expression. - Any proactive measure must be subject to rigorous human rights risk assessment, implemented with narrowly tailored scope, transparency, and meaningful recourse options to ensure proportionality and accountability.
0	**Preventative Measures**	**P8**	**Friction**			No KYC requirement for identifying and mitigating suspicious registration and domain usage activity via risk-based model for post-registration	NIS2 Cooperation Group guidelines on Article 28 implementation & Infermal Study	Perpetrators are able to establish bogus online presences to advance abusive behavior before corrective action is taken	

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						identity verification			
0	**Preventtive Measures**	**P9**	**Practices that are prone to abuse**	X (could be a best practice ?)		Economic incentives (discounts) are more prone to DNS abuse	INFERMAL	Discounted pricing is strongly correlated with an increase in malicious registrations.	RrSG • this goes toward individual actions by Contracted Parties related to fraud-mitigation; each has a different business model and so a different solution and we must be allowed to continue to have that flexibility. • unclear if ICANN can regulate pricing RySG feedback : • Discounted pricing is strongly correlated with growth in TLDs. Just because malefactors use a feature does not make that feature bad, especially when it's important for acceptable registrants. More data is needed to understand what, if

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									anything, is to be done here. NCSG (Re: Domain Pricing & Access) - Affordable or free domain names are essential for digital inclusion. They allow individuals, small businesses, and civil society groups to establish a presence online. - Pricing should not be used as a blunt tool for abuse mitigation. Doing so risks disproportionately harming legitimate users and undermining efforts to expand equitable access to the Internet. - Abuse mitigation by registrars offering low-cost domains should instead rely on rights-respecting measures: clear abuse reporting channels, prompt investigation, proportionate

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									response, and strong due process—not financial barriers. Farzi: - Even if that is the case, considering people's access to domain name is at stake, we should not base any of our recommendations on this finding. CSG feedback: - ICANN is only an occasional price regulator and should not generally be required to regulate retail pricing. - Economic incentives between ICANN and contracted parties would be a more sensible approach; e.g., an economic reward for decreasing namespace abuse. At-Large

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									-Requiring change of business model (discounts, "bulk registrations") are not fruitful. Identify "bad actors" and focus on these should be prioritised. -Cheap or free services can attract bad actors who want to set up abusive domains with little cost or risk, but the answer isn't to get rid of discounts altogether — it's to make sure registrars do proper checks and close any loopholes that let abuse slip through. -If Registrars had meaningful registrant verification safeguards (i.e. email and phone validation + identity verification) these other issues would be largely irrelevant. -While there may be high correlation further work is required to determine whether these are real

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									causes of abuse. **Majority think gaps under Theme 7 have to be addressed through policy, if at all attempted
0	**Preventative Measures**	**P10**	**Practices that are prone to abuse**	X (could be a best practice ?)		Free services are more likely to be abused by threat actors	INFERMAL	Services like free hosting and privacy shield attackers from costs and detection.	RrSG • this goes toward individual actions by Contracted Parties related to fraud-mitigation; each has a different business model and so a different solution and we must be allowed to continue to have that flexibility; we also note well the existence of the picket fence." • unclear if ICANN can impose registrars to charge for ancillary services Farzi: - They also enable people who don't have access to financial services and lack resources to have access to

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									domain names. This not only helps with human rights, it also helps with incentivising people to have their own websites instead of going on social media platforms At-Large - see gap 6
0	**Preventative Measures**	**P11**	**Associated domain check**			Limited Use of Abuse Data for Preventive Action	INFERMAL	Abuse feeds data is not consistently used to inform domain-level restrictions or validation rules.	RrSG • Abuse feed sata can be outdated or incorrect - *should* it be consistently used? • retail blocklists are typically low-value (they are in the business of finding abuse, not of mitigating abuse, so are often outdated; they often are funded by rights-holders so are overbalanced toward names that involves rights-related abuse; some charge a fee for removal post-mitigation; there are

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									hundreds of thousands of lists—and they have value for certain purposes; the value of lists can also vary over time); Contracted Parties may use multiple feeds to enrich each other and give us better data but it's not something that should be put into a PDP or enforced in any way. • Additional Info: This study confirms that's not the best method https://seclab.skku.edu/wp-content/uploads/2025/05/3696410.3714678.pdf RySG feedback : • Does not agree this is a gap as described [section 6.6, section 8] • Certain features may be desirable to phishers, those same features are also desirable by ordinary registrants. It seems like

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									this item is emphasizing the former point at the cost of ignoring the latter point, with no data to support whether or not those features are used predominantly by malefactors. At-Large (High Priority) • Limited use of abuse feeds data for preventive action highlights a significant gap in cybersecurity practices • Underuse reduces effectiveness of early detection and response and failing to integrate abuse data into proactive defense strategies is missed opportunity to flag/block abuse/harm CSG: - There are many sources of abuse data. Get

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									community-wide input on what's useful and reputable and integrate appropriately. Using only "favored" feeds is unfairly dismissive.
1	**Abuse Reporting**	**A1**	**Complainant reports**	RySG: ICANN Compliance to address, not a subject for policy work		25% of unactionable abuse complaints, Best Practices for Reporting Phishing, Unsure of Where to report	ICANN Org Report on DNS Abuse mitigation requirements (Nov 2024)	Lack of proper complaint data or understanding results in ICANN closing complaints without action. Many complaints are closed due to missing or inadequate evidence, like lack of URLs in screenshots or failure to respond to follow-up requests. Phishing is the most common category of DNS Abuse and often	RrSG • ICANN is welcome to use the guide that CPH have created • Contracted Parties have produced a number of examples of how to correctly report DNS Abuse; we are happy to allow ICANN to help us socialize them RySG feedback : • Gap in ICANN process, appropriate for “process improvement” but not appropriate for consensus policy work Farzi - This can be easily

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
								misreported. The CPH/CSG abuse reporting workshop at ICANN 82 revealed there's still much room for improvement on how to report phishing to registrars (and registries when appropriate). Phishing reports that are incomplete, or incorrectly evidenced, create a bottleneck in contracted parties anti-abuse team's queues — Actionable reports contribute to reducing	overcome through asking for the documents, and evidence and not allowing for the complaint to be submitted if incomplete CSG feedback: - The community has been doing tutorials for more than a year. It's educated the ICANN community but tutorials at ICANN meetings and sporadic online guides won't resolve the issue. - Frivolous complaints of course are just that. Non-frivolous but legitimate complaints that perhaps aren't formatted to over-exacting standards deserve action. RrSG: see response to G15 • ICANN could takeover acidtool.com or build their own solution. It's not apolicy issue.

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
								mitigation times overall.	RySG feedback : • For consideration: SAC115 provides context on reporting to the appropriate channels for adequate mitigation — i.e., escalation paths. That said, consensus policies can only affect those under ICANN contracts. Hosting providers are outside the area of influence. • Reporters send abuse reports to registrars and registries because it is easier than sending reports to other parties e.g., website owner, hosting provider, etc. • Not a subject for policy work. ALAC (High Priority) • Ability for end-users to report DNS abuse quickly and effectively is a foundational – clear

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									guidelines on reporting channels and requirements would help victims to effectively inform about abuse cases • Consistency in reporting requirements whichever channel used should improve quality of complaints • NetBeacon Reporter and 2024 DNS abuse contractual amendments have only partly helped TO NOTE: Reporting tools, processes and education must be sufficiently simple, take note of language barriers, lack of technical savviness / knowledge of what constitutes DNS Abuse ADDITIONAL GAP: Requirement to inform complainant of outcome of complaint

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									At-Large - Addressing Gap 27 will to some extent also address Gap 17 Farzi: Under what circumstances and who should fix this problem? Sometimes the domain name points to a cloud space and they have their own abuse handling mechanism. Obviously that is outside of ICANN's mission. We can come up with the specific cases that we can actually help and we should be clear who should be involved. Sometimes browsers are better than giving warnings. CSG feedback: - There always will be inefficient or misdirected abuse reports to registrars. Not everyone will see your

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									guidelines in their moment of need. - How about a policy requirement for publishing a "how to report abuse" tutorial resulting from a community-wide cooperation group on improving instruction, including useful details on where to report certain kinds of abuse?
1	**Abuse Reporting**	**A2**	**Mitigation Information From Contracted Parties**			Measurement challenges due to 'uncategorized' domains	NetBeacon Blog Analysis (2024) - Impact of ICANN Contract Amendments	Unclear outcomes hinder evaluation of DNS abuse mitigation effectiveness.	RrSG • in many cases, the DNS Abuse is reported to multiple levels (hosting company, registrar, email provider, registry, …) and any of them might take action; some retail block lists provide mitigation reports (note that URLs are not domains and so counts can be difficult to measure); we encourage a data-driven approach to Policy

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									• we additionally look forward to additional data and reporting from law enforcement • They are many sources OpenPhish, APWG, Malware Patrol, and URL Abuse are some of them. Mitigation can be measured. It's harder to know who took action registrar/registry/CDN/hosting etc. but it's possible to measure. At-Large • See Gap 22
1	**Abuse Reporting**	**A3**	**Compromised vs Malicious**	RySG: Not a subject for policy work		Lack of clarity between malicious and compromised domains, Limited	DNS Abuse Small Team Report (2022) NetBeacon Blog Analysis (2024) - Impact of	The report suggests distinguishing between malicious vs. compromised registrations when considering what topics may	RrSG: see response to G19 RySG feedback : • For consideration:TopDNS' DNS Abuse Table: https://international.eco.de/download/205700/ illustrates which actors

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						impact on compromised domains	ICANN Contract Amendments	fall within the scope of ICANN to address. Taking this approach would ensure that responsibility for taking action on malicious registrations is within the remit of Contracted Parties and/or ICANN org, while action on compromised registrations may require involvement of actors that are not subject to ICANN agreements.	—within the internet ecosystem— may be best positioned to mitigate a certain online harm. It may help to disambiguate (or help in the discussion) as to the scope of ICANN policy. At-Large From an individual end-user's perspective, both malicious and compromised domains pose equal levels of risk — phishing, malware, fraud, or data theft — but compromised domains are often more deceptive because they appear trustworthy. Users are more likely to click on links from known or legitimate websites, making these threats harder to detect and more dangerous. Currently, most DNS abuse mitigation efforts focus on

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									maliciously registered domains, leaving compromised domains under-addressed (Gap 19). This leaves a major gap in protection, especially as hijacked domains are increasingly used in sophisticated attacks. Additionally, the lack of a clear distinction between malicious and compromised domains (Gap 24) leads to confusion in ownership of mitigation responsibilities — registrars, hosting providers, and registrants often point fingers. This slows response time, increasing the window of harm for users. Clarifying definitions and response protocols would ensure faster mitigation, regardless of domain origin, and significantly improve end-user safety.

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									RrSG • we support differentiation between compromised domains and those maliciously-registered • Most of the time, the domain name isn't compromised; the website it points to is. The criminals are not getting access to the registrant account on the registrar platform. They gain access to the hosting/CMS." RySG feedback : • Not a subject for policy work. • “Overlooks” is a mischaracterization, suggestion to reframe gap description to “compromised domains are not studied. • “While abuse related to compromise is still a

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									concern, typically the registry and registrar are not well-placed to appropriately mitigate harm (especially at scale) related to compromised websites because of the potential for collateral damage." At-Large -While the distinction between malicious and compromised domain names is a valid concern, the priority needs to be on identifying all abuse, including the 25% not being fully reported. -Compromised domain names are a problem for end-users because they are often unaware that they are compromised rather than registered with bad intentions. There needs to be education on this.

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									Compromised domain names exploit the credibility of the domain name. Additional Gap: Lack of early-warning systems for compromised domains / real-time alerting mechanism (e.g., browser warnings or DNS-level blocking) that could prevent widespread harm. Insufficient support for legitimate domain owners to recover from compromise.
3	**Contractual Obligations (Well-positioned party takes action as necessary**	**C1**	**Mitigation Information From Contracted Parties**			Limited transparency in reporting on DNS Abuse mitigation actions taken	NetBeacon Blog Analysis (2024) - Impact of ICANN Contract Amendments	Lack of detailed mitigation reporting reduces accountability and oversight.	RrSG: see response to G13 RySG feedback : • This should be a question to Compliance on whether it is able to get what it needs when reviewing compliance. • Possible security

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									questions regarding reporting actual mitigation actions. • There is a clear distinction to be made here between knowing that “an action was taken” and “knowing the action taken”. At-Large (High Priority) • If there’s no clear measurement or transparency, no one really knows if DNS abuse is being properly handled. For Gap 18, when domains stay ‘uncategorized,’ it’s hard to track what threats are most common or how well mitigation is working. For Gap 22, if registrars and registries don’t clearly report what actions they take, it reduces trust and accountability ADDITIONAL GAP:

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									• Absence of standardized reporting formats across contracted parties, no public access to aggregated abuse mitigation data, and lack of third-party audits to verify the accuracy of reported actions CSG feedback: - This is a legitimate shortcoming. We also advocate for documenting back to the abuse reporter action taken on instances of contractually defined abuse.
3	**Contractual Obligations (Well-positioned party takes action as necessar**	**C2**	**Associated domain check**			No requirement to investigate associated domains,	NetBeacon PDP Whitepaper INFERMAL CSG/CPH ICANN81	Registrars are not required to check for other domains linked to malicious activity, allowing abuse to persist across multiple domains.	RrSG • must differentiate between retail and wholesale registrars (and potentially other types of registrars) to accommodate the business needs of all registrars • how will it be enforced?

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									At-Large (High Priority) - Significant gap in domain abuse prevention using pattern of abuse - Lack of obligation to examine associated domains allows patterns of abuse to persist and spread; undermines broader efforts to secure DNS and enabling cybercriminals to exploit loopholes - Some CPs already do this so making this a policy is sensible NCSG (re: Associated Domains & Surveillance) - When investigating actionable DNS abuse, registrars may need to examine other domains associated with the same registrant data to disrupt broader abuse networks. However, such inspections

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									must be conducted with strict safeguards to avoid undue surveillance of legitimate registrants. Investigations must be grounded in clear, specific evidence of abuse linked to the registrant—never on speculative or broad profiling. The focus must remain on the abusive activity, not on surveilling the registrant's broader online presence. Farzi - Associated domains check could have a profiling impact. what are the safeguards to avoid that? CSG (High Priority) - Continuing to act on "one-off" abuse reports by individual domain is the most inefficient way to report and resolve abuse. Registrars are in a position

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									to mitigate abuse before it occurs with this measure. RrSG: see response to G3 • Implementation and enforcement will be really difficult. • Registrars/registries will have to prove a negative if they did not find any abusive name linked to the reported one. And if one or more newly reported domains happen to be associated with the previous one later, what will the consequences be? It may easily lead to the creation of blacklists that registrars will have to implement to forbid the registration of domain names using certain details/payment information etc. Furthermore, if those details are too specific and

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									published, the criminals will have a blueprint for avoiding the obstacles registrars are implementing. At-Large • See Gap 1, should merge Gap 1 and Gap 30
3	**Contractual Obligations (Well-positioned party takes action as necessary)**	**C3**	**Dispute resolution**			No standard recourse mechanism for registrants	NetBeacon PDP Whitepaper, NSCG Human Rights Session at ICANN83	Registrants lack a formal process to contest domain suspensions, risking harm from erroneous actions?	RrSG • we support published recourse mechanisms for registrants to appeal to a registry for a registry-level suspension • publication by registrars of how to lodge a complaint for a registrar suspension is reasonable RySG feedback : • Dispute resolution should be part of the whole abuse mitigation policy at a basic level. Given the level of false positives in reports and fake/AI generated

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									evidence being submitted in reports definitely leads to inaccurate actions on the part of the mitigating body. This can be easily addressed by making it mandatory for registries and registrars to have a 'dispute' form or an 'unsuspension' request form right next to the abuse reporting form on their websites. NCSG: - Post-Mitigation Remedy & Recourse Registrars must maintain accessible and transparent mechanisms for registrants to seek remedy or challenge decisions. This includes: - Restoration Process: A pathway for legitimate registrants to demonstrate that abuse has been resolved—or that the action

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									was mistaken—and regain control of their domain in a timely manner. - Complaints & Appeals: A clear and fair process through which registrants can file complaints or appeal mitigation actions, reinforcing procedural fairness and accountability. CSG feedback: - A reasonable appeal process makes good sense. **At-Large** -Absence of a formal mechanism to contest suspensions increases the risk of harm to registrants—especially if the system is not transparent, lacks accountability, or makes mistakes. Introducing a clear, fair, and timely

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									appeals process would be essential for trust and balance in domain abuse mitigation. -From an end-user perspective, the suspension of a domain — especially one that provides essential services like healthcare, education, financial access, or communication — can cause significant disruption. If a domain is suspended in error and the registrant has no clear or timely recourse, users are the unintended victims, losing access to critical services or information without explanation or recourse themselves. Moreover, unjustified suspensions without transparency can erode public trust in the DNS ecosystem and abuse mitigation frameworks. A standardized, transparent,

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									and accountable recourse mechanism ensures that legitimate domains can be restored quickly, reducing harm to users while still enabling effective action against true abuse. Fairness for registrants and reliability for end-users are deeply interconnected.
3	**Contractual Obligations (Well-positioned party takes action as necessary)**	**C4**	**Pass down requirements to registrants**			Unregulated subdomain abuse	NetBeacon PDP Whitepaper	Registrants offering subdomain services are not required to mitigate abuse, creating an oversight loophole?	RrSG • a domain is a domain; abuse on a subdomain is abuse on the domain and the registrant is responsible. • ICANN should not make a difference between domain names and subdomains. The registrant is always responsible. That's a slippery slope. Many providers are offering subdomain names as part of their service (icann-community.atlassian.

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									net/ for example), ICANN cannot regulate them, let alone registrars who only have a contractual relationship with registrants. At-Large (High Priority) • No requirement for registrants offering subdomain services to monitor or report abuse, lack of verification for subdomain resellers, and no standardized best practices for subdomain management – gaps allow abuse to persist under otherwise reputable domains.
3	**Contractual Obligations (Well-positioned party takes action as necessary)**	**C5**	**Impostor domain names**			No requirement to mitigate exact match to	ICANN81 Joint Session CPH & CSG	Exact match domains are used for phishing, disinformation and other	

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						known identity or trademarked terms		fraudulent activity	
3	**Contractual Obligations (Well-positioned party takes action as necessary)**	**C6**	**Pre-Mitigation Due Diligence**			Before taking any mitigation action, registrars must carry out thorough and proportionate due diligence based on specific, actionable evidence. This helps prevent false positives and ensures	NCSG Email		

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						that mitigation measures are appropriate to the verified abuse. Where possible, less restrictive alternatives should be considered before resorting to domain suspension.			
3	**Contractual Obligations (Well-positioned party takes action as necessary)**	**C7**	**During Mitigation Transparency**			When action is taken against a domain, the registrant	NCSG Email		

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						must be promptly notified (laws to the contrary might apply, we are not talking about those circumstances) This notice should include: - The reason for the action; - The type of action taken; - The initiator of the action (e.g., registrar,			

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						third-party request); - A clear explanation in accessible language.			
3	**Contractual Obligations (Well-positioned party takes action as necessary)**	**C8**	**Industry coordination**			Similar complaints receive differing responses at inconsistent times; standardisation of reponses from registries and registrars is sought.	BC NetBeacon White Paper	Inconsistent or non-substantive responses and timing lead to inefficient mitigation steps and needless follow-up requests	
Community Collab	**Community Collaboration**		**Industry coordination**			Mitigation of Batch Registered	Workshop on CPH Ideas for	Cybercriminals and botnet operators use a	RrSG • we support registries working together with law

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
oration						Domain Names Generated by a Botnet Algorithm	Future Work on DNS Abuse	DGA or Domain (Name) Generation Algorithm to create a large number of domain names they can use to launch cyber attacks, including some forms of DNS Abuse. Criminals may use API-based registration tools to register the DGA names. To counter these threats, there are special purpose organizations that analyze a DGA to extract the list of domain names, including a corresponding activation date.	enforcement and with ICANN to minimize the impact of DGAs as they are better-situated that registrars are to combat this particular type of DNS Abuse; we reiterate our support for recourse mechanisms for registrants with domains affected by registry action At-Large • Gap 5 and Gap 32 can be merged

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
								This information is not widely spread and maybe hard to vet at scale for registries or registrars to act upon. Opportunity: Develop an operational framework to provide (all) gTLD registry operators with a verified list of botnet generated domain names to prompt proactive action at scale.	
4	**Enforcement (Effective enforcement by ICANN Compliance if**	**E2**	**No requirement**	RySG: Not a subject for		No Sanctions or Deterrents for	ICANN Org Report on DNS Abuse mitigation requiremen	While formal breach notices exist, there is no clear policy for escalating	RrSG • we encourage ICANN Contractual Compliance to use the tools they have been provided to enforce

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
	appropriate action is not taken by Contracted Parties)			policy work		Recurring Non-Compliance	ts (Nov 2024)	sanctions for habitual offenders unless contractually breached multiple times.	the contract • What is missing? A way to terminate the RAA faster? RySG feedback : • This seems like an ICANN procedural issue, not a policy issue. At-Large (High Priority) • Effective enforcement is the backbone of DNS abuse mitigation. • When enforcement is inconsistent (Gap 13), slow (Gap 20), or lacks real consequences for habitual offenders (Gap 15), the abuse environment thrives — directly harming users through phishing, fraud, and malware. Moreover, ambiguity in contract language (Gap 29) like “reasonable” or “prompt” allows for delays and minimal action – weakens

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									trust in registrars and in ICANN's compliance framework. • Vague contract language allow registrars to delay/avoid action w/o consequences. • Addressing Gaps 15 and 29 should have an effect on Gaps 13 and 20 • 2024 DNS abuse contractual amendments are only partly helpful ADDTIONAL GAPS (wrt Contractual Compliance and CPs) • Requirement to inform complainant of outcome of complaint • More transparency in action/enforcement outcomes CSG feedback: - If 2024 amendments were sufficient, the community

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									wouldn't have continued to raise the issue and form this small team. - Agree with ALAC regarding vague language that allows dishonorable registrars too much latitude. - The community has raised for years the idea of graduated penalties vs. only breach warnings on the way to termination. Now is a good time to consider.
			NEW INPUTS BELOW 3 July 2025						
4	**Enforcement (Effective enforcement by ICANN Compliance if appropriate action is not taken by**	**E3**	**No requirement**	RySG: Not a subject for policy work		Delayed ICANN enforcement actions	NetBeacon Blog Analysis (2024) - Impact of ICANN Contract	Slow issuance of breach notices reduces deterrent effect of contractual obligations.	RrSG: see response to G15 • Considering the delay in ICANN compliance replies, if this timeframe is reduced, compliance time to answer will have to reset the clock." RySG feedback :

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
	Contracted Parties)						Amendments		• This seems like an ICANN procedural issue, not a policy issue. At-Large • See Gap 15
4	**Enforcement (Effective enforcement by ICANN Compliance if appropriate action is not taken by Contracted Parties)**	**E4**	**Practices that are prone to abuse**	RySG: Not a subject for policy work		Abuse concentrated in a small number of registrars	NetBeacon Blog Analysis (2024) - Impact of ICANN Contract Amendments	Some lesser-known registrars are disproportionately targeted for abuse. identifying what are the factors that lead to this	RrSG: see response to G15 RySG feedback : • Seems like a compliance problem, not a policy problem. At-Large -Gap 21 is tied to ICANN Contractual Compliance enforcement -Lack of registrar accountability for abuse originating from promotional campaigns matters
4	**Enforcement (Effective enforcement by ICANN**	**E5**	**No requirement**			No suitably rapid time to mitigation,	ICANN81 Joint Session CPH & CSG	DNS abuse is propagated in minutes or hours, requiring more	

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
	Compliance if appropriate action is not taken by Contracted Parties)					leaving abuse to unfold and persist. 24 hour response time requested for reported instances of abuse (as defined by RAA)		timely mitigation and response	
4	**Enforcement (Effective enforcement by ICANN Compliance if appropriate action is not taken by Contracted Parties)**	**E6**	**No requirement**			No requirement to "close the loop" regarding correctly submitted reports of abuse with documentation of	ICANN81 Joint Session CPH & CSG	Abuse reporters unaware of steps to mitigate abuse and uncertain if action was taken	

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						resolution to reporter			
Community Collaboration	**Community Collaboration**	**CC1**	**Industry coordination**			Inefficient coordination on DGA-based abuse	NetBeacon PDP Whitepaper, Workshop on CPH Ideas for Future Work on DNS Abuse	Law enforcement must individually contact registries, causing delays in malware/botnet mitigation. Cybercriminals and botnet operators use a DGA or Domain (Name) Generation Algorithm to create a large number of domain names they can use to launch cyber attacks, including some forms of DNS Abuse. Criminals may use API-based registration tools	RrSG: see response to G32 At-Large (High Priority) • No single trusted platform or protocol for real-time information sharing between registries, registrars, hosting providers, and law enforcement means fragmentation causing delays and inconsistent responses. • Insufficient collaboration with global CERTs and ISPs to halt impact of cross-border abuse Standardized threat language and classification system would improve accuracy & speed. • Absence of registrar-to-registrar abuse intelligence sharing, so

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
								to register the DGA names. To counter these threats, there are special purpose organizations that analyze a DGA to extract the list of domain names, including a corresponding activation date. This information is not widely spread and maybe hard to vet at scale for registries or registrars to act upon. Opportunity: Develop an operational framework to provide (all) gTLD registry operators	abusers often hop between registrars once action is taken TO NOTE: Gap 5 and Gap 32 could be merged RrSG • we support registries working together with law enforcement and with ICANN to minimize the impact of DGAs as they are better-situated that registrars are to combat this particular type of DNS Abuse; we reiterate our support for recourse mechanisms for registrants with domains affected by registry action At-Large • Gap 5 and Gap 32 can be merged

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
								with a verified list of botnet generated domain names to prompt proactive action at scale.	
Community Collaboration	**Community Collaboration**	**CC2**	**Industry coordination**			No requirement to periodically update abuse definitions; establishment of CCWG for consistent review of DNS abuse definitions is necessary.	SSR2 Recommendations (10.2) SAC115	Per SAC115: "...no particular list of abuse types will ever be comprehensive." This leaves users exposed to non-mitigation of new types of threats.	CSG feedback: - SAC115 does not defines dns abuse. Since, abuse is ever-evolving; as DNS stewards, it makes sense to periodically review the definition, as SSR2 and SSAC have recommended.
Data & Transparency	**Data & Transparency**	**DT1**	**Industry coordination**			Little transparency regarding abuse-relat	BC	Lack of transparency slows ICANN Compliance	

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
						ed trends by registry / registrar; community reporting would add transparency and focus to enforcement efforts.		enforcement work and causes public confusion	
Data & Transparency	**Data & Transparency**	**DT2**	**Lack of research /data**			Lack of empirical research on abuse factors	INFERMAL	Not much research comprehensively quantified the impact of registrar/TLD features on malicious domain registrations.	RrSG: see responses to G14, G18 At-Large -ICANN needs far better data in support of policy development and implementation. -Without reliable data, we can't design effective policy. Users are left unprotected if key abuse patterns or mitigation gaps are unknown. -Without solid data, it's

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									hard to know what's working and what isn't. For Gap 8, more research would help everyone understand what factors really drive abuse — and fix them at the source. -Unless research is able to provide unassailable conclusion, it will always be subject to challenge. -ICANN is not a research organisation. It needs to deal with these data deficits. The industry is often much better than academia at collecting and analysing some of this data because their business is on the line. Academia tends to be trying to understand problems that may have been fixed years ago. There needs to be more cooperation.

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
Data & Transparency	**Data & Transparency**	**DT3**	**Lack of research /data**			ICANN has no overview of mitigation actions taken outside the contract enforcements.	ICANN Org Report on DNS Abuse mitigation requirements (Nov 2024)	No overview on overall DNS Abuse (mitigation) landscape.	RrSG • we encourage data-driven approaches to Policy • 3.18.4 is already in place. It's a matter of how to implement it. (full disclosure, we do not sort abuse reports as a category, they are attached to the domain name(s) they pertain to. I suppose it's the case for the majority of the industry, this would require development cost and time) At-Large -If ICANN doesn't have the full picture of how abuse is actually being handled outside formal enforcement, it's tough to spot gaps, share what works, or build trust that abuse is really being dealt with. -There are probably 3rd party entities that can do

Phase	Lifecycle Category	(New) Gap ID	Theme/ Cluster	Not In Scope For Policy-Making	Already addressed (maybe partially)?	Gap Description	Document/ Source	Why is it a gap? (according to source document)	Small Team Comments
									overview research a lot better than ICANN can. -The overview of mitigation actions is important to stop people wasting time on a problem that has already been fixed. Additional Gaps: -ICANN does not collect or report metrics about user impact (e.g., financial harm or loss of access) from DNS Abuse. This limits visibility of real-world consequences. -Lack of user-centric impact data on DNS abuse (e.g., financial loss, trust erosion), limited data sharing among stakeholders, and no standardized metrics to evaluate mitigation effectiveness across registrars and TLDs.

Annex B – DNS Abuse Small Team Assignment Form

The DNS Abuse Small Team Assignment Form can be found here and below:
https://gnso.icann.org/sites/default/files/policy/2025/draft/assignment-form-gnso-council-small-team-dns-abuse-04apr25-en.pdf

ICANN | GNSO
Generic Names Supporting Organization

GNSO COUNCIL SMALL TEAM – WORK ASSIGNMENT OVERVIEW

Subject	**DNS Abuse**
Background	The topic of DNS Abuse was revisited during ICANN82 as a potential area for future policy work. It had previously been addressed by a **DNS Abuse Small Team**, which had produced a set of **four recommendations and** identified a gap in enforcement mechanisms under current contracts. Contract amendments between ICANN and contracted parties were negotiated to clarify mitigation obligations. Now that those amendments have taken effect and related data from ICANN Compliance is available, the Council proposed to revisit the issue. **Key Inputs and Developments** 1. **Contractual Amendments & Compliance Report**: ICANN Compliance presented data assessing the effectiveness of the new amendments that enhanced enforcement of DNS Abuse responsibilities in registry and registrar agreements. 2. **INFERMAL Study**: A study (Inferential Analysis of Maliciously Registered Domains) offered insight into attacker behavior in domain name abuse and was considered a valuable input. 3. **Small Team Recommendations**: In November 2022, the Council passed a motion accepting the recommendations as outlined in the DNS Abuse Small Team report. These had been previously adopted by Council with a motion specifying that Recommendation 1 (discussing a potential issue report on malicious registrations) would proceed only after completing Recommendations 2–4 (focused on collaboration, outreach, and engagement). 4. **ICANN Domain Metrica: A Measurement Platform:** Six years ago, ICANN launched the Domain Abuse Activity Reporting (DAAR) system. It was intended to stimulate discussion around Domain Name System (DNS) abuse and serve as a reliable and reproducible measurement methodology to help registrar and registry operators to monitor DNS abuse. ICANN Metrica was built as a follow-up system that does a lot more with the data ICANN has available; it forms a new framework and a measurement platform that meets ICANN needs and the needs of the wider community. The first module will include aggregated and non-aggregated data on DNS abuse concentrations as listed on a set of Reputation Block Lists (RBLs), similar to what DAAR had, but this time for both registrars and registries. This should give users access to more detailed and relevant information about DNS abuse concentration patterns.
Assignment	The Small Team is tasked to: • Evaluate broader DNS Abuse mitigation efforts across ICANN (e.g., by the CPH, other community groups, and potentially industry firms focusing on DNS abuse). Consider whether briefings from such groups would aid the small team. Similar to the first

ICANN | GNSO
Generic Names Supporting Organization

	iteration of the DNS abuse small team, conduct outreach to the community, seeking their input on items specifically suitable for policy development.
	• Assess the impact of the Contract amendments on DNS abuse mitigation efforts.
	  ○ Is more information/data needed from compliance when discussing the next steps?
	  ○ Are the current mitigation efforts addressing DNS abuse sufficiently? If not, seek to identify gaps that would be best addressed via policy development.
	• Discuss and provide a summary on the insights from the INFERMAL study and how these insights can help inform next steps on DNS abuse.
	
	Expected Outcome:
	• A report to GNSO Council including:
	  ○ Findings from review of available data sources;
	  ○ List of gaps the Small Team may have identified;
	  ○ Recommendations to GNSO Council on next steps on what other work (policy, further research, etc.) might be needed to address DNS abuse.

Timing	6-8 months to 1) Review existing data available 2) Perform outreach to the community 3) Consider that input and identify next steps 4) Draft report for the Council.
Members	Sam Demetriou (RySG) Bruna Martins (NCSG) Vivek Goyal (BC) Justine Chew (ALAC) Jennifer Chung (RySG) Farzaneh Badii (NCSG) Lawrence Olawale-Roberts (BC) Sebastien Ducos (RySG) Greg Dibiase (RrSG) Paul McGrady (NomCom) Thomas Rickert (ISPCP) Peter Akinremi (NCSG) Desiree Milosevic (NomCom)
Documents	DNS abuse small team final report INFERMAL Study ICANN Compliance 6-months report on DNS abuse mitigation requirements
Notes	See background section
Next Steps	• GNSO Council to consider the assignment.