Namecheap, Inc
4600 E Washington Street, Suite 305
Phoenix, Arizona 85034

Namecheap, Inc., Public Comment: Preliminary Issue Report on a Policy Development Process on DNS Abuse Mitigation

17 October 2025

Namecheap, Inc. appreciates the opportunity to comment on the GNSO Council's Preliminary Issues Report on a Policy Development Process on DNS Abuse Mitigation (Report). We recognize all the work and effort of the ICANN Policy Support Staff in drafting this Report.

DISCUSSION:

Namecheap generally supports the three issues identified in the Report as being prioritized for policy work in the near future. It is imperative that each issue be addressed in a separate "Micro-PDP" with separate charters. It will be best to conduct them one at a time, in order to make sure all necessary parties have a chance to participate and each issue is given the full attention and resources of the community.

We also strongly encourage the focus on the proposed PDPs to remain very narrowly scoped to ensure that the PDPs (and implementation) can truly be done in an expedited[1] manners. The issue of combatting DNS Abuse is an important one for the ICANN community to consider, and these PDPs should not resemble so-called "Christmas tree bills" in the United States, which have many additions and amendments that distract from the main focus of the legislation. Although the ICANN Community will likely submit suggestions for expanding these PDPs, we strongly recommend that any suggestions outside of the Report be deferred for future policy work. Completing these Micro-PDPs successfully and quickly can demonstrate that the ICANN Community can indeed be agile when addressing important matters.

While Namecheap strongly encourages broad, diverse, and open ICANN community participation in these policy efforts, we would like to caution the community: bad actors are listening. The Registrar Stakeholder Group's Abuse Contact Identifier (ACID) (located at acidtool.com) has been subject to cyberattacks (1) within days of first being publicly announced

[1] Namecheap notes that these should be PDPs and not EPDPs. The term "expedited" in EPDP is unfortunate because EPDPs only skip a step (the Issues Report) but do not otherwise proceed in a faster manner. This has led many in the community to criticize the speed of EPDPs. It is hoped that by having very narrowly scoped Micro-PDPs, they can proceed in a manner that the community would consider to be "expedited".

at ICANN76 and (2) when substantial improvements were announced at ICANN83. There have been no identifiable attacks at any other time since its launch in 2023. Any discussions and specific recommendations need to be as general as possible to ensure that bad actors cannot easily find workarounds thus defeating the hard work of the community. For example, if a PDP on API access focuses on ten or more domains, then bad actors would use nine. For the PDP on associated checks, if a detailed list of all possible items that registrars should consider and review are discussed or appear in any recommendations, bad actors will ensure multiple associated accounts have differences sufficient to avoid being noticed. The PDPs should strive to find a balance on creating meaningful obligations but ensuring that registrars can consider items not detailed in resulting policies to ensure that the resulting Consensus Policies have long-term applicability.

Namecheap additionally supports the RrSG's comments regarding representation on the PDP Working Groups, which as currently proposed do not ensure adequate representation of registrars. There are many different registrar types, including wholesale and retail, which have vastly different operational models. Registrars also vary in size from thousands of domains under management (DUMs), to hundreds of thousands, to millions of DUMs. There are over 3,000 accredited registrars in almost all regions of the world. It would be impossible for two registrar members to be able to speak competently and representatively on behalf of all registrars, and they would need to consult outside of the PDP within the RrSG to ensure that all voices are adequately heard. By increasing registrar participation to ensure diversity of registrar models, the PDPs (two of which in large part will only create obligations for registrars) can proceed faster and fairly.

Additionally, Namecheap supports the Public Comment from the Contracted Party House DNS Abuse WG and the RrSG as indicated in this comment.

1. **Unrestricted Application Programming Interface (API) access for domain name registration for new customers:**

Namecheap supports prioritizing the API issue for initial policy work and recognizes that many registrars already have established processes that include gating or friction to reduce incidents of abusive behavior. This would be similar to the DNS Abuse amendments which created a floor for all registrars based upon the efforts of most registrars that prioritize reducing abuse on their platforms. Having these requirements in a Consensus Policy will ensure that all ICANN-accredited registrars are required to provide basic or minimum controls for API access or face compliance actions.

2. **Associated Domain Checks:**

Namecheap supports policy work that would establish certain obligations on registrars to conduct a holistic investigation of the registrant's account, including checking whether other domains in the account have been flagged for abuse or other fraud. These checks should be conducted in a manner that adheres to data privacy principles, confidentiality, and due process (especially for any review and enforcement by ICANN Contractual Compliance). Finally, this

should only focus on maliciously registered domains rather than compromised ones to ensure that legitimate sites are not targeted.

3. **Limited coordination on Domain Generation Algorithm (DGA)-based abuse: Botnets**

Namecheap supports the creation of a centralized trusted hub to make sure the responses by registries are coordinated and swift when required in urgent abuse cases. We are not opposed for ICANN to take that role; however, Namecheap believes that this process does require a narrowly scoped PDP, instead of the recommendation in the Report that this can be done outside of the contractual requirements. The goal should be to ensure that *all* gTLD registries are required to participate in these efforts, and a voluntary effort *will not* ensure this outcome. The 2024 DNS Abuse amendments to the RAA and the RA and this issues report are in direct response to registrars and registries that were not following industry best practices, and allowing the DGA issue to be considered outside of ICANN policy efforts would guarantee that *not all* gTLD registries would participate thus not fully addressing the issue.

Preventative Measures (Phase 0)

Namecheap appreciates the gaps that the Report identifies. Please see our additional comments below. We are also happy to note that the Report highlights the need for balance when establishing preventive measures by considering the need for an open and accessible domain name marketplace.

P1: Unrestricted Access to Application Programming Interface (APIs) allowing for high-volume registrations

Namecheap supports the RrSG's feedback on P1. We additionally caution that by providing specific details, limits, or exact requirements into a public ICANN policy will allow bad actors to easily circumvent the policies and continue their campaigns unimpeded and without recourse for the ICANN community to address without additional policy work.

P2 and P3: Lack of Proactive/Timely Contact Verification:

Namecheap supports the RrSG comment to extend an invitation to the SSAC to provide or endorse tools for basic syntactic checks (email and phone formats per RFC).

Namecheap does not support any additional policy work on this topic as we already have adequate requirements in the RAA and Consensus Policies. If research identified registrars that were not conducting the appropriate contact verification requirements in the RAA (which has been in place since 2013), and is the only RAA available to gTLD registrars, then the matter should be referred to ICANN Compliance rather than creating additional policy work which could punish the vast majority of registrars that are fully compliant with the requirements of the RAA. It should also be noted that there are situations where contact verification is not required (e.g. RDDS Accuracy Program Specification (RAPS) Section 3), so additional details regarding claims of untimely contact verification are required to assess alleged non-compliance.

P5. Minimal Deterrent Effect of Reactive Measures ("Uptime"):

Namecheap supports the RrSG comment and agrees that "this gap does not appear to warrant any specific solution".

P6. Challenges in Real-Time Detection of Short-Lived Abuse:

Namecheap supports the RrSG comment.

P7. Underuse of Predictive Algorithms for Early Detection:

Namecheap supports the RrSG comment and will actively participate in drafting a best practices document as described in the RrSG comment. It should be noted that although predictive algorithms may assist with the identification of maliciously registered domain names, they often result in false positives which could subject innocuous domains to suspension. Such predictive algorithms are not a panacea, and additionally are subject to the constantly changing approaches by bad actors exploiting the DNS for criminal activity.

P8. No Post-Registration Identity Checks for Suspicious Activity:

Namecheap supports the RrSG comment. We reiterate that Registrars already have contractual obligations that address this issue, and we do not support any additional policy efforts.

Namecheap additionally notes that verification of identity does not stop or prevent DNS Abuse, and there is no evidence to support this notion. It is a costly approach that will accomplish little (if anything). If this were to become a requirement, bad actors will engage in additional identity theft and human trafficking to ensure a steady supply of "verifiable identities". There are already readily available methods to easily obtain "verifiable identities"[2] and there are reports of individuals selling identity verification to bad actors on black markets in China. The ccTLD .cn is often cited as a model for advocating identity verification, however as of 17 October 2025, Spamhaus ranks the .cn ccTLD as the third most abused ccTLD in the world.[3]

P9. and P10. Economic Incentives Prone to Abuse (P9 - Discounted Pricing and P10 - offering Free Services):

Namecheap does not believe that minimum pricing is within ICANN's remit and should be ultimately left for the contracted parties to decide on how to address. Additionally, creating minimum pricing levels could harm domain name registrants by artificially increasing the price of domain names (especially for those in underserved regions or with limited budgets). Domain

[2] https://cybersecurityasia.net/cloudsek-exposes-china-linked-counterfeit-id/

[3] https://www.spamhaus.org/reputation-statistics/cctlds/phishing/

names should be available for registration by anyone regardless of means, and abuse can be addressed through non-pecuniary methods.

P11. Limited Use of Abuse Feeds/Threat Data for Prevention:

Namecheap supports the RrSG comment. Additionally, it should be for individual contracted party to determine which of these commercial (e.g. paid) services they should utilize, based upon the registrar or registry's unique business needs. Namecheap notes that some popular abuse feeds contain high levels of false positives and little (if any) transparency regarding data collection and analysis. Requiring contracted parties to use these services may result in additional work for contracted parties and the suspension of many tens of thousands of innocent domain names annually (including those related to governments and critical infrastructure).

Abuse Reporting (Phases 1–2)

Namecheap agrees with the Report's statement that successful abuse mitigation depends on the efficient flow of information: a well-evidenced report sent to the correct party will facilitate prompt review and mitigation of abusive activity.

A1. Unactionable Complaints to ICANN:

Namecheap is well aware of all the unactionable reports ICANN receives and is appreciative of ICANN's efforts to filter those out. We are very supportive of educating the public and ICANN staff on what makes a good report, and are willing to assist with these activities from the unique perspective of our team (with over ten years of combined experience working for ICANN Contractual Compliance and also the same at a domain registrar).

A3. Malicious vs. Compromised - Clarifying Responsibility:

Namecheap supports the RrSG comment.

Taking Action on DNS Abuse (Phase 3: Contractual Obligations)

Namecheap was co-lead for the RrSG negotiation team for the 2024 DNS Abuse Amendments and continues to support ICANN Compliance's efforts to use the tools they were provided to pursue registrars that do not comply with the new requirements.

C1. Limited Transparency in Mitigation Actions taken:

Namecheap supports the RrSG comment, and especially encourages the Staff and the Community to focus on developing policy for high-impact areas, taking into consideration limited resources.

C2. No Requirement to Check for Associated Domains:

Namecheap supports a PDP regarding associated domain names, however as noted above, the details regarding what checks and processes are available to registrars should not be discussed in detail in public. Frequently, associated malicious domains are not in the same customer account, and may require additional resources to discover.

Contract negotiations with ICANN are confidential, and will ensure that registrars can be very detailed in what methods and manners registrars can undertake to determine whether a maliciously registered domain name is associated with other domain names or accounts. Namecheap, however, supports the CPH commitment to participate in the policy process for additional work on DNS Abuse after the DNS Abuse Amendments. If possible, we would propose or support closed or (otherwise confidential) discussions within the ICANN Community and ICANN org to ensure additional information sharing without providing a guide to bad actors to circumvent the good efforts of the Community to take additional action to reduce DNS Abuse.

C3. Lack of Standard Dispute/Recourse Mechanism for Registrants:

Namecheap supports a PDP that will provide a recourse mechanism for registrants upon domain suspension or any mitigation actions taken by registries or registrars. This issue warrants a separate PDP; however, we do feel like this should not be one of the first PDPs on this topic.

C4. Unregulated Subdomain Abuse:

Namecheap supports the RrSG comment.

C6 and C7. Due Diligence and Transparency in Mitigation:

Namecheap supports the RrSG comment and reiterates the report's findings that these considerations do not necessarily represent a gap in DNS Abuse mitigation.

C8. Inconsistent Responses - Seeking Standardization:

Namecheap supports the RrSG comment and reiterates that the Amendments did not include rigid timelines to provide flexibility in addressing DNS abuse, that as we know vary in complexity.

Enforcement by ICANN Contractual Compliance (Phase 4)

E2. No Clear Escalation of Sanctions for Recurring Non-Compliance:

Namecheap does not have any feedback on this section.

E3. Delayed ICANN Enforcement Actions:

Namecheap does not have any feedback on this section.

Community Collaboration (Cross-Cutting)

CC1. Lack of Coordination during Domain Generation Algorithm (DGA) Botnet Attacks:

Namecheap does not have any feedback on this section.

CC2. No Mechanism to Update DNS Abuse Definitions (Periodic Review):

Namecheap does not have any feedback on this section.

Data & Transparency (Cross-Cutting)

P4. Lack of Data on "Bulk Registrations":

Namecheap notes that there is a lack of data on so-called "bulk registrations" because there is no accepted definition of "bulk registrations". Some in the community have mentioned five- which is a ridiculously small number and would cause widespread registrant frustration across the DNS. Additionally, the term "bulk registration" does not consider batched registrations for resellers, could impact large portfolio purchases (e.g. a brand owner registering fifty domains for an upcoming product launch), domain investor purchases, and there is no evidence that reducing "bulk registrations" would stop DNS Abuse. Additionally, if a threshold is identified, bad actors would immediately reduce volume per session, use different accounts, or use different registrars, to ensure they could continue their campaigns.

Namecheap notes that increasing API friction for unrestricted API access will be more effective in reducing abusive domain name campaigns, while ensuring legitimate large portfolio registrations can continue.

DT2. Lack of Empirical Research on Abuse Factors:

Namecheap does not have any feedback on this section.

Consideration for a PDP:

Namecheap supports narrowly scoped targeted PDPs for the three issues identified in the Report. One of the potential PDPs identified is Associated Domain Checks**,** which can be a first Mini-PDP that will immediately have an impact on DNS Abuse. Having a narrowly scoped PDP will allow the community participants to focus on one issue that can be addressed expeditiously. We recognize staff's concerns over limited resources, which is why we support

consecutive PDPs instead of conducting them concurrently.[4] It is important that all necessary parties can participate, and having consecutive PDPs will allow subject matter experts to participate and provide input on all identified issues.

Tackling and implementing Associated Domain Checks will give us the time and space to focus on the other two issues identified as preventative measures, the API and DGA.

Namecheap agrees with the Report's identification of Unrestricted API Access and Associated Domain Checks as the two priority topics. We do not agree that the coordinated mitigation of DGA-Based Botnet Domains should be addressed outside of policy development as discussed above. We strongly support a narrowly scoped PDP for this priority issue as well and would ask that staff add this issue to consideration for the PDP.

Thank you for your time and consideration of this feedback.

Sincerely,

Owen Smigelski
Head of ICANN Compliance and Relations
Namecheap, Inc.

[4] It may be possible for ICANN to stagger several PDPs so that certain phases, such as the Working Group, Implementation Review Team, or public comment periods overlap without conflicting and overtaxing resources. Namecheap encourages ICANN org to be creative with determining timelines to achieve maximum efficiency and speed while ensuring full community participation.