

Identity Digital Inc.
Public Comment on the Preliminary Issues Report on a Policy Development Process on DNS Abuse Mitigation

Identity Digital Inc. is the parent company of the registry operators of over 270 gTLDs, provides registry services to over 160 gTLDs and ccTLDs, and provides retail registrar services through its subsidiary name.com. We appreciate the opportunity to provide feedback to the GNSO Council on the Preliminary Issue Report on a Policy Development Process on DNS Abuse Mitigation (the “Preliminary Issues Report”).

We applaud the GNSO Council and, in particular, the GNSO Small Team on DNS Abuse (the “Small Team”), for swiftly identifying DNS Abuse mitigation gaps and calling for the Preliminary Issues Report to be drafted. We also express our appreciation for the hard work and careful analysis provided by the ICANN staff members who authored the Preliminary Issues Report.

We agree with the Preliminary Issues Report that the first two gaps identified by the Small Team - unrestricted application programming interface (API) access for domain name registration for new customers and associated domain check - should be the first priority for policy development. However, we think the decision to include both topics in a single policy development process (PDP) is wrong. Since the beginning of discussions of DNS Abuse-related PDPs, the ICANN community has agreed that any proposed PDPs must be narrowly scoped and achievable, and that any proposal that attempts to address a number of topics would take too long and potentially lead to stagnation. By addressing each of the identified gaps as a separate PDP, the GNSO Council can ensure participants have the most relevant experience, remain focused on one issue, and achieve meaningful change in ICANN policy related to DNS Abuse mitigation.

The GNSO Council should move swiftly to initiate a PDP addressing the associated domain check gap and prepare to initiate a PDP on unrestricted API access for domain name registration for new customers immediately following the GNSO Council’s approval of the recommendations from the first PDP.

While preventing DNS Abuse by requiring registrars to add restrictions to their registration APIs will slow the creation of new malicious domains, more immediate action is appropriate in addressing the DNS Abuse that is currently occurring. A requirement that registrars who receive a well founded report of a malicious domain engaged in DNS Abuse review other domains registered at the same time, or held in the same account, for similar abusive behavior will help ensure registrars address DNS Abuse at scale and end the constant whack-a-mole that so often is DNS Abuse reporting and mitigation.

Identity Digital is supportive of a representative model for any PDP resulting from this Issues Report. Therefore, we strongly believe that among the GNSO constituent groups, representation should be equal at the Stakeholder Group level. As currently proposed, the Commercial Stakeholder Group is allotted up to six seats on the Working Group, while the Non-Commercial Stakeholder Group, the gTLD Registries Stakeholder Group (RySG), and the Registrar Stakeholder Group are each only allotted two seats. This is far from representative.

The Preliminary Issues Report identified the third Small Team gap, better coordination in addressing Domain Generation Algorithm (DGA) attacks, as possibly addressable outside of the policy development process. We encourage ICANN to begin a dialogue with the RySG, country code Name Supporting Organization (ccNSO), and law enforcement on measures ICANN can take outside the policy development process to improve coordination among these groups in addressing DGA attacks. The GNSO Council should remain apprised of those discussions and revisit whether policy development is appropriate or necessary as those conversations develop.

Identity Digital looks forward to continuing to work with the GNSO Council and the broader ICANN community to advance policies that effectively mitigate DNS Abuse while maintaining a stable, secure, and resilient internet.