NABP
National Association of Boards of Pharmacy

847/391-4406
Fax: 847/375-1114

1600 Feehanville Dr
Mount Prospect, IL 60056
help@nabp.pharmacy

TO: New gTLD Subsequent Procedures PDP Working Group Leadership

FROM: Gertrude "Gg" Levine, Digital Health Manager, on behalf of National Association of Boards of Pharmacy

DATE: 15 January 2021

RE: Minority Statement

National Association of Boards of Pharmacy appreciates the work done by the New gTLD Subsequent Procedures PDP Working Group and supports all the recommendations in its final report. However, we have concerns with Recommendations 9.1 and 9.3. To be clear, we do not oppose the recommendations; rather, we believe that as written they represent a scant minimum standard of conduct by responsible registry operators. These recommendations should go further to ensure that registry operators support the security and stability of the DNS. This includes supporting public safety and establishing trust in gTLDs. Actionable public Interest Commitments (PICs) are critical to establishing trust in gTLDs, as they set out expectations for responsible registry operator conduct.

Recommendation 9.1

We support Recommendation 9.1 as it recommends that Specification 11 3(a)-(d) of the current Base Registry Agreement continues to be included in the Base Registry Agreement as a minimum standard. However, we are concerned that the current language of Specification 11 3(a) does not adequately support the goal of preserving and enhancing the security and stability of the DNS. A critical aspect of ensuring the security and stability of the DNS is establishing trust in gTLDs. Specification 11 3(a), however, falls short of that goal in that it only mandates that registries include in their Registry-Registrar Agreements specific language. It does not require contractual enforcement of the safeguards described in that language.

Some uses of domain names, such as those described in Specification 11 3(a), can directly undermine the security and stability of the DNS, for example distributing malware, abusively operating botnets, phishing, and engaging in fraudulent or deceptive practices, counterfeiting, or other activity contrary to applicable law. Registry operators must operate responsibly by ensuring that their registrars require that their registrants do not use their domain names to undermine the security and stability of the DNS. The language in the Base Registry Agreement needs to reflect this obligation and expectation of responsible registry conduct.

Recommendation 9.3

We support the inclusion and formal adoption of Category 1 Safeguards as policy for future rounds of new gTLDs. We believe Category 1 Safeguards play an important role in applying protections to strings related to highly sensitive or regulated industries in two ways. First, they establish trust in those strings associated with the industry by maintaining existing regulatory obligations online in the relevant gTLD space(s). Second, by applying relevant regulatory obligations for registrants, the registry operator

supports and furthers the public safety goals envisioned by the regulation. However, the concern with lack of enforceability we set out above also applies to the language used in Registry Agreements to include Category 1 Safeguards. As with Specification 11 3(a), Specification 11 3(e)-(g), (i), (j), and (l) only require Registry Operators to include specific language in their Registry-Registrar Agreements.

Moving forward, we believe that future implementation of these policy recommendations should include language in the Base Registry Agreement that more clearly articulates the expectations of responsible registry operators. Such expectations should set out actionable commitments that support public safety and trust in gTLDs, which ultimately strengthen the security and stability of the DNS.