Sarah B. Deutsch
Vice President and Associate General Counsel
Verizon Communications Inc.

1320 North Court House Road
9th Floor
Arlington, Virginia 22201

Phone 703 351-3044
Fax 703 351-3669
sarah.b.deutsch@verizon.com

February 27, 2012

Re: Request for Comments on Defensive Applications for New gTLDs

Verizon appreciates the opportunity to submit comments on the issue of defensive applications for new gTLDs. ICANN has long heard from a broad array of stakeholders about how the new gTLD rollout would unnecessarily drive defensive-based decisions and increase costs on parties who have no interest or desire to own a top level domain or police for infringement, fraud and abuse at the second level. We believe the risk of defensive registrations at the second level is much higher than the risk of defensive applications at the top level. We urge ICANN to issue a second comment period to hear from the community specifically about continuing concerns at the second level. Because this period may represent our only chance to comment on this issue, we will address defensive behaviors on both levels.

As an initial matter, we take issue with the phrasing of the fundamental question posed in the RFC, asking why "*some* stakeholders *recently* indicated that they are concerned about the *perceived* need for defensive applications at the top level." We disagree with the characterization of stakeholder concerns about defensive applications/registrations as only to applying to "some," and as being "recent" or as merely "perceived." In fact, trademark owners, business organizations, nonprofits, IGOs and a host of entities and individuals have consistently raised such concerns throughout the new gTLD process. The phrasing implies some surprise on ICANN's part. ICANN, in fact, was not only well aware of the concerns, but shoulders some of the responsibility for driving this "perceived need for defensive applications." ICANN Board members widely touted the opportunity for trademark owners to apply for a .brand as their best defense against cybersquatting, fraud and consumer confusion. On a larger scale, ICANN's extensive roadshow (and parallel marketing efforts by those with financial interests to sign up applicants) marketed the new gTLDs as a unique "opportunity," possibly limited in time, with little up-front transparency about who could be applying to register a .brand, and possibly leading to an expensive auction process at the back end. It is therefore not surprising that many in the community are still concerned about the need for defensive registrations.

Consistent with our prior filings throughout the DAG process, we offer the following comments on actions ICANN could still take today to decrease the risks of defensive behavior at the top level, but, even more importantly, at the second level. As discussed in Verizon's numerous DAG comments, the existing RPMs ICANN characterizes as a "suite" are so diluted to provide almost no protection for trademark owners to address the inevitable wave of cybersquatting, fraud and abuses in the new gTLDs. We urge ICANN to consider, before it is too late, the following constructive ideas to provide real remedies to the business, trademark and nonprofit communities:

Limited Beta Test

Verizon supports the idea of a limited beta test. A narrowly crafted beta test would allow ICANN to test the operational aspects of expanding the new gTLD system and could be used to measure the volume of cybersquatting, fraud and abuse, along with the effectiveness of the proposed RPMs. For example, a beta test could be limited to 30 new gTLDs, such as ten Internationalized Domain Names, ten generic TLDs and ten geographic/regional names. Stakeholders would be less inclined to engage in unnecessary defensive filings if they understood that ICANN was opening a spigot rather than a fire hydrant, and testing the system slowly and responsibly for unintended consequences.

Create a "Do Not Register" List at the Top and Second Levels

Just as ICANN reserved its own name and considered those of the Red Cross and the Olympics to be off limits as new gTLDs, all trademark owners should also have a one-stop "opt out" option at both the top and second levels. The ICM registry, the registry of the .xxx TLD, offers a variation of this remedy today at the second level. There could be a small one-time fee to opt out from having one's trademark included across all the gTLDs. The list would be maintained by ICANN's proposed "Trademark Clearinghouse" and available to trademark holders who submit proof of a national trademark registration and other requirements to supplement their trademark information. Registries would need to check the list and decline any registrations that run up against the names on the list. In the case of disputes, there could be an administrative process similar to a UDRP, where a party could challenge a particular name on the list. This list is not the same as a "Globally Protected Mark List." Governmental organizations, IGOs, and nonprofits should all have the right to make use of the do not register option.

The Do Not Register List would prevent cybersquatters from registering domain names that are identical to registered trademarks but would also include domain names that include additional words along with trademarks. The recently publicized incidents of speculation and cybersquatting following the rollout of the new .xxx gTLD should be instructive to ICANN when it considers the "perceived" concerns of brand owners. Even though Verizon paid a high fee for the privilege of *not* registering the VERIZON brand in the .xxx gTLD, this did not prevent third parties from paying an expensive application fee to register variations of Verizon.xxx. For example, a cybersquatter immediately registered Verizonwireless.xxx and attempted to auction it off on a third party website. This incident highlights a few points. First, that cybersquatting, fraud and abuse are not speculative. They continue to take place in the existing gTLDs and will occur in new gTLDs. Real remedies are needed on the front end. The ICM registry policy should be one model ICANN examines to craft a rigorous trademark protection program. Second, although a Do Not Register list is an imperfect remedy, it is at least one step that arguably prevents a party from applying for their own name at the top level, but more importantly (for the vast majority of trademark owners) at the second level. Third, the existing RPMs proposed in the DAG would not prevent or adequately address these abuses (see discussion of RPMs below).

Strengthen Existing Rights Protection Mechanisms

ICANN has consistently failed to heed the recommendations made by the IRT, brand owners, IGOs and many others. Instead, ICANN offers a watered down version of the IRT recommendations. These so-called remedies will wind up substantially raising costs for brand owners and result in a need to rely on old remedies to enforce in thousands of new gTLDs at the second-level. These RPMs take up many pages in the DAG, but when examined even briefly, amount to overly burdensome, risky and expensive proposals. Trademark owners can only safely rely on the existing trademark remedies already used by brand owners, such as the UDRP or civil remedies available under the ACPA, neither of which scale or necessarily are available to address the volume of infringement that will occur at the second level.

We urge ICANN to sure up the proposed RPMs by:

(a) Amending the Post-Delegation Dispute Process to offer real remedies against new registries that become havens for cybersquatting, frauds and other crimes. There should be a lower the standard of proof from the "clear and convincing evidence" threshold to a more reasonable preponderance of evidence standard. Registries should be held accountable when acting in bad faith and with willful blindness for fraudulent and illegal activities that are shown to arise on a continued basis in their delegated gTLD.

(b) Adopting the ideas discussed in our prior DAG comments on ways to improve the Trademark Clearinghouse. As noted in our prior comments, the "sunrise period," by definition, is nothing more than an expensive form of defensive registration at the second level. ICANN did not adopt our recommendation to limit the price on sunrise registrations, which further drives up the costs for needless defensive registration at speculative prices. The Trademark Claims service is not a "remedy" for the many reasons we discuss in our prior comments.

(c) Encouraging and working with law enforcement to strengthen an accurate WHOIS, not just through "Thick WHOIS."

(d) Reforming the URS into a meaningful remedy. As discussed in our prior comments, the proposed URS creates only uncertainty and risk for brand owners. At a minimum, amend the URS to (1) include a transfer remedy that will provide brand owners with the ability to avoid perpetual monitoring obligations and reduce the risk of a domain name later falling into the hands of another cybersquatter; (2) lower the standard of proof from clear and convincing evidence to a preponderance of the evidence as in the UDRP; (3) remove any requirement that a URS provider make any substantive determination about how a trademark owner is "using" its mark; and (4) implement a real "loser pays model" that applies regardless of how many domain names one registers in bad faith. If the URS cannot be offered for $300 as proposed by ICANN (and we suspect no legitimate provider can offer it as

this price), ICANN should consider having its registrars implement a notice and take down process. Without substantial changes that transform the paper process into a real remedy, only the expensive options of a UDRP or possible ACPA suit remain as viable choices for trademark owners.

Strengthen and Reinforce Registry and Registrar Contractual Responsibilities

Verizon looks forward to reviewing the new RAA provisions when they become public. We would hope the new RAA would require registrars and registries to place provisions in their terms of services that allow for sufficient discretion to address cybersquatting and abuse when advised of illegal activities. We support stronger WHOIS authentication, especially where domain names are registered through a "privacy service" and immediately reveal the registrant's contact details to the trademark owner in the case of infringement or other illegal activities. Registrars who register domain names on their website should warn potential registrants who search for a new domain name using a "domain name spinner" search tool that the name they are searching may be similar to a third party's trademark and have them acknowledge when registering a domain name that they are not violating the trademark rights of third parties.

Conclusion

As structured today, unfortunately, ICANN's proposed new gTLD process may result in defensive behavior by those who wish to register and use a gTLD and those who do not. Brand owners who feel that they may lose out to another brand owner using the identical mark but for unrelated goods and services may feel pressured into filing. And all brand owners, including those who decide not to file, will still incur unnecessarily high costs to protect their brands and their consumers from frauds and abuses at the second level.

In sum, defensive behaviors – either at the top level or second level – would only confirm the unaddressed flaws in the new gTLD program. Defensive registration at any level is the opposite of ICANN's stated goal to drive innovation, "competition and choice by introducing new gTLDs into the Internet's addressing system." Without immediate and significant changes to the gTLD program, the only "choice" left to ICANN stakeholders will be to engage in the non-innovative defensive behaviors that are the subject of this public comment period.

Thank you again for the opportunity to provide these comments and we are happy to discuss any of these ideas in greater detail.