August 27, 2013

Board of Directors
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Re: ICANN Proposal to Mitigate Name Collision Risks

Dear Members of the ICANN Board:

This public comment is submitted in response to ICANN's request on August 5, 2013, for community comment on ICANN's proposed efforts to mitigate potential impacts resulting from name collisions as new gTLDs are delegated into the root zone as described in the "New gTLD Collision Risk Mitigation" proposal published that same day.

***Introduction***

Faced with growing evidence of broadly recognized name collision risks and potential SSR issues arising from a premature delegation of new gTLDs into the root zone, including advice from ICANN's own Security and Stability Advisory Committee ("SSAC"), ICANN has now presented its "New gTLD Collision Risk Mitigation" proposal that, if implemented, would shift the responsibility to ensure the stability and security of the DNS to hundreds of new gTLD applicants after delegation and activation of new gTLDs into the root zone. Under its proposal, ICANN would effectively wash its hands of the security concerns and the operational, technical or financial responsibility to address them. We believe this shift of responsibility undermines ICANN's core mission and conflicts with ICANN's Articles of Incorporation, Bylaws, Code of Conduct and its contractual commitments under the Affirmation of Commitments ("AoC") with the United States Department of Commerce. Further, we believe ICANN is best positioned to mitigate the risks of naming collisions. ICANN, and not the applicants, should bear the financial costs and retain the legal and reputational risks associated with possible naming collisions.

***ICANN's Risk Mitigation Proposal Transgresses ICANN's Governing Documents***

Following its creation, ICANN immediately assumed the responsibility to ensure that all of its decisions were guided by the need to preserve the stability and reliability of the Internet, an obligation identified by the U.S. Government in its 1998 White Paper as "the first priority of any

DNS management system."[1] In its first report to the U.S. Department of Commerce ("DOC"), ICANN made the primacy of this obligation clear: "In particular, ICANN agrees with the White Paper's assertions that 'the stability of the Internet should be the first priority'[.]"[2] The White Paper also made it clear that this responsibility was particularly acute in the context of any decisions to delegate new TLDs into the root zone, noting that "a prudent concern for the stability of the system suggests that expansion of gTLDs proceed at a deliberate and controlled pace to allow for evaluation of the impact of the new gTLDs and well-reasoned evolution of the domain space." ICANN also accepted this particular responsibility from its inception, agreeing in the original Memorandum of Understanding with the DOC that the process to consider the possible expansion of the number of gTLDs should, first and foremost, "consider and take into account . . . the potential impact of the new gTLDs on the Internet root server system and Internet stability."[3]

ICANN's primary obligation to ensure that all of its decisions, including any decisions to delegate new TLDs into the root zone, preserve and enhance the stability and reliability of the DNS, is reflected throughout its own governing documents. ICANN's Articles of Incorporation list "promoting the global public interest in the operational stability of the Internet" as one of the primary purposes of the newly formed Corporation.[4] Both ICANN's Bylaws and its Board of Directors' Code of Conduct establish ICANN's mission as "to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems." Finally, ICANN's Code of Conduct establishes "preserving and enhancing the operational stability, reliability, security and global interoperability of the Internet" as the first core value that "should guide the decisions and actions of ICANN."[5]

In addition to the obligations set forth in other governing documents, ICANN's AoC with the U.S. Department of Commerce establishes a contractual requirement for ICANN to ensure that any security, stability and resiliency issues are adequately addressed prior to the implementation of any decision to delegate new gTLDs into the root zone. Specifically, Section 9.3 of the AoC requires ICANN to "ensure that as it contemplates expanding the top-level domain space, the various issues that are involved (including competition, consumer protection,

---

[1] "Statement of Policy on the Management of Internet Names and Addresses" 63 Fed. Reg. 31741, 31749 (1998) (the "White Paper") (available at http://www.gpo.gov/fdsys/pkg/FR-1998-06-10/pdf/98-15392.pdf)
[2] First Status Report to the Dept. of Commerce, Section III, dated June 15, 1999 (available at http://www.icann.org/en/about/agreements/mou-jpa/statusreport-15jun99-en.htm)
[3] Memorandum of Understanding between the U.S. Dept. of Commerce and the Internet Corporation for Assigned Names and Numbers, Section (V)(C)(9)(a) (Nov. 25, 1998) (available at http://www.ntia.doc.gov/other-publication/1998/memorandum-understanding-between-us-department-commerce-and-internet-corporat)
[4] Articles of Incorporation for the Internet Corporation for Assigned Names and Numbers, Section 3 (Nov. 21, 1998) (available at http://www.icann.org/en/about/governance/articles).
[5] Bylaws for Internet Corporation for Assigned Names and Numbers, Art. 1, Section 1. (April 11, 2013) (available at http://www.icann.org/en/about/governance/bylaws); ICANN Board of Directors' Code of Conduct (May 6, 2012) (available at http://www.icann.org/en/groups/board/governance/code-of-conduct).

security, stability and resiliency, malicious abuse issues, sovereignty concerns, and rights protection) will be adequately addressed prior to implementation."[6]

It is therefore completely understandable that ICANN's Applicant Guidebook ("AGB") for new gTLDs places responsibility for security and stability of the DNS upon ICANN itself. Section 2.2.1.3, for example, describes ICANN's procedure to study and test in the Initial Evaluation process each new gTLD string to ensure it does not cause instability to the DNS. The Interisle Consulting Group, coincidentally, appears to have been retained by ICANN to perform the DNS stability evaluation on a string by string basis. Interisle published in June 2013 the stability evaluation criteria and concluded that no string would pass this review if it did not comply with relevant standards or if it would "adversely affect the throughput, response time, consistency, or coherence of responses in Internet servers ***or end systems***." If we now know that "end systems" are likely to be damaged, ICANN must be accountable and responsible for its decision to approve each of the impacted strings.

Consistent with its mission and purpose, and with the AGB, we submit that the risks arising from name collisions (and other security and stability risks) should be mitigated by ICANN, and not applicants, and should be completed *prior to* delegation of any new gTLDs. An ICANN administered risk mitigation regime, pre-delegation, will ensure a consistent, coherent and uniform mitigation approach. In addition, ICANN indisputably has collected sufficient funds to conduct this risk mitigation activity and has obtained sufficient legal protections from applicants and others.[7]

***Applicants are Not Positioned to Perform Risk Mitigation***

Unfortunately, despite its mission and governing documents, and the DNS stability review noted above, ICANN has proposed to shift the entire burden of mitigating the risks associated with naming collisions to the new gTLD applicants. Under ICANN's proposal, applicants are obligated to detect potential naming collisions, to provide notice to impacted parties, and to offer "customer support" to these parties. These burdens and obligations belong to ICANN and cannot and should not be shifted to applicants.

First and foremost, ICANN's approach will not yield a consistent and effective risk mitigation program. Applicants will each develop different notice and notice techniques and will offer varying levels of "customer support." For example, some experienced applicants could be in position to provide remediation advice to impacted parties, but other applicants, with less technical experience, will not. Furthermore, under ICANN's plan, an applicant could learn though its notice program that many end users will experience harm once the new gTLD is activated. Nevertheless, ICANN imposes no requirement to mitigate the harm prior to delegation. Worse, under ICANN's plan, the applicant is not required to even tell ICANN that it

[6] Affirmation of Commitments, Section 9.3 [emphasis added].
[7] Letter from R. Goshorn to J. Jeffrey dated June 14, 2013.

has learned during the notice and customer support functions that the new gTLD string will be harmful to end users. The applicant may simply proceed to activation without any further steps. We do not believe ICANN's plan is likely to lead to effective notice or mitigation.

Moreover, while ICANN has been on notice since at least 2009 that these kinds of risks were possible, and, as noted above, retains sufficient funds to remediate the harm from its new gTLD program, applicants who applied for the new gTLD strings were completely unaware that ICANN would shift these costs and the associated risks to them. We believe that ICANN's proposal creates substantial new legal risk to applicants and we believe these risks should be borne by ICANN and not shifted to the applicants. For example, should ICANN's proposal be adopted, applicants will have a duty to provide notice of possible risks arising from the activation of the new gTLD. Applicants who fail to effectively perform this duty will face increased legal exposure should the activation cause harm or damage to parties unaware of the potential risks. Similarly, ICANN's proposal requires that applicants provide "customer support." It is likely that some applicants do not have sufficient expertise to perform this task appropriately. Any failure to provide effective assistance could substantially increase an applicant's legal exposure if end user systems are damaged by ICANN's new gTLD string. Further, ICANN's plan shifts the reputational harm that might arise to applicants even though ICANN itself established the new gTLD program and established the Initial Evaluation criteria, and it has been ICANN that has approved each and every string for delegation. It is therefore ICANN, and not individual applicants, who should bear the legal risks and reputational harm that might arise from the notice and mitigation.

***Conclusion***

We believe ICANN's risk mitigation proposal should be rejected. The proposal if adopted would undermine ICANN's mission and other governing documents by shifting the obligation for ensuring security and stability of the DNS to new gTLD applicants. Further, ICANN's proposal would not create a unified and consistent risk mitigation regime and would be unlikely to be effective. Finally, ICANN should not be permitted to shift the costs and risks, both legal and reputational, to applicants. ICANN has the remit, is best positioned and has the funds to address naming collision mitigation. ICANN should retain responsibility for addressing naming collision mitigation and should bear the associated risks and costs from any failures in this regard.

Sincerely,

Patrick S. Kane
Senior Vice President, Naming Services
VeriSign, Inc.

Richard H. Goshorn
Senior Vice President, General Counsel
& Secretary
VeriSign, Inc.