September 17, 2013

Dr. Steven Crocker
Chair, Board of Directors
Internet Corporation for Assigned Names and Numbers

Mr. Fadi Chehadé
President and CEO
Internet Corporation for Assigned Names and Numbers

Mr. Cherine Chalaby
Chair, Board New gTLD Program Committee
Internet Corporation for Assigned Names and Numbers

Dear ICANN Board of Directors,

The undersigned companies and organizations submit this letter to express our significant concern regarding several unresolved stability and security issues associated with the upcoming delegation of new gTLDs. We understand that the New gTLD Applicant Group (NTAG) recently submitted a letter on these issues. While some of the undersigned are members or observers of NTAG, we disagree with NTAG's position on these issues, and are submitting this letter to accurately reflect our views.

Over the last several years, ICANN's Security and Stability Advisory Committee (SSAC) has correctly identified several critical issues that demand attention, mitigation or resolution prior to delegating new gTLDs into the root. These issues have been formally and publicly recorded in SSAC reports to the ICANN Board (SAC045, SAC046, SAC057, and SAC059) but they have not yet, unfortunately, received the necessary levels of attention and focus from the ICANN Board and Staff and the broader community. These concerns were recently acknowledged, in part, by ICANN's August 5, 2013 posting for public comment of the Interisle Consulting Group naming collision study and ICANN staff's accompanying proposed mitigation strategy.

These issues must be addressed to preserve the stability, security and resiliency of the DNS. Allowing known risks to remain unresolved would be irresponsible and inconsistent with ICANN's core mission. It is crucial that ICANN's leadership recognizes and works with the appropriate technical bodies to ensure these issues and risks are defined, evaluated, and addressed comprehensively. This is of particular concern to operators of Internet infrastructure whose networks and customers will be negatively impacted. The cost to business of transferring known risks to unknowing end users is substantial and must be avoided.

As described by the SSAC and verified by the recent Interisle study, the delegation of new strings that are already widely in use as internal identifiers in enterprise, government, and other private networks into the root of this multi-billion user ecosystem will present substantial security risks. If and when delegations occur, these naming collisions will cause breakage in existing networks, negatively impacting enterprises, governments, and end users who are unaware of the source of the problem.

These issues are not new. In fact, since the early "Scaling the Root" studies in 2009, there have been recommendations for further study and assessment of these problems. We are now at a critical point.

Unexpected name collisions caused by new gTLDs being delegated into the root could have devastating consequences. For example, if .corp is delegated into the zone as a new gTLD, it is possible that thousands or tens of thousands of enterprises could be impacted. However, the problem is not just with obvious widely-used strings like .corp; even strings that have small query volumes at the root may be problematic, such as those discussed in SAC045. These "outlier" strings with very low query rates may actually pose the most acute risks because they could support critical systems and services. Any such negative impacts may have serious consequences for those who rely on the DNS, and this should raise significant liability concerns.

To minimize the transfer of risk and potential harm to business and consumers, devices and infrastructure of the Internet, we believe it is critical for ICANN to make a concerted effort to avoid the risks, but to also alert potentially impacted parties through a meaningful education and outreach program. We therefore request an update on ICANN's definitive resolution of these political and technical risks as we approach the program's most critical decision point.

We are very troubled by the proposed recommendation of ICANN staff to transfer sole responsibility for these critical outreach efforts to new registry operators, when, in fact, the responsibility is ICANN's. As such, we view ICANN's proposed mitigation strategy as inadequate. As has been iterated for the past three years by ICANN advisory committees, ICANN must work with the community, including providers of Internet infrastructure and services -- not just new gTLD applicants -- to directly and urgently communicate these known risks to potentially impacted parties, prior to any delegations.

These issues are critically important to the stability of the DNS. Solutions and/or effective mitigation plans must be developed and widely implemented prior to delegation to preserve trust in the Internet. ICANN must work with enterprise users of the DNS, with ISPs, who provide DNS services to both commercial and non-commercial users, and with other impacted parties to review the collision-related stability and security impacts of every new gTLD. Furthermore, ICANN must be prepared to defer the introduction into the DNS of any new gTLD that the review identifies as presenting a stability and security threat. Such deferrals should remain in effect until those threats can be substantially eliminated.

We are available to cooperate with ICANN and the community to help define and resolve these challenges, so that the introduction of new gTLDs can occur in a timely and responsible manner. We respectfully request a reply to this joint letter.

Sincerely,

David Tennenhouse
Corporate Vice President, Technology Policy
Microsoft Corporation

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

J. Scott Evans
Head of Global Brand, Domains & Copyright
Yahoo! Inc.