



August 8, 2013

Ms. Vernita D. Harris
Senior Telecommunications Policy Specialist
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave, NW,
Room 4701
Washington, DC 20230

Dear Ms. Harris,

Thank you for your August 2, 2013, response to our May 30, 2013, letter regarding the security and stability concerns that we and others believe could be introduced by the upcoming delegation of new gTLDs.

With regard to our public statements addressing the introduction of delegations of new gTLDs into the root zone, it is important to differentiate between “ability” and “advisability.” While we have the ability today to add the mutually agreed upon 100 TLDs to the root zone per week, we and others believe that it is prudent to take a more cautious approach to adding records to the root zone at least until appropriate safeguards, particularly those recommended by the Security and Stability Advisory Committee (SSAC), are in place. Further, as you are aware, Verisign has a duty specified in the Cooperative Agreement between Verisign and the Department of Commerce to serve the public interest in the continued security and stability of the Internet domain name system (DNS).¹

On the question of advisability, it is important to make clear that Verisign is not the first and is not alone in expressing concerns over security issues raised by the introduction of new gTLDs. The National Research Council, in a 2005 report “Signposts in Cyberspace,” warned that introducing new TLDs into the root at a rate exceeding “tens of TLDs per year” would risk

¹ Cooperative Agreement, Am. 30, Section 2 A (ii).

instability.² ICANN's own SSAC, as well as expressly commissioned study teams of experts, issued several advisories, dating back to 2009, advising ICANN to take steps prior to introducing new gTLDs.³ The lack of implementation of these recommendations was documented in SAC059, issued April 18, 2013, which included clear language on the lack of progress and additional work needed.⁴ While we believe an equitable rollout for new gTLD applicants is possible, this can only be achieved with a deliberate and measured deployment.

Additionally, both the At-Large Advisory Committee (ALAC)⁵ and the Governmental Advisory Committee (GAC) have written to ICANN's board of directors advising them to heed SSAC advice on dotless domains and name collisions, and to make SSAC analysis public.⁶ We believe we are providing precisely the value that both ICANN and the Department of Commerce sought in their agreements with us – security and stability advice from the most experienced operator of the largest and historically the most reliable registry, thus leveraging a broad base of institutional knowledge and subject matter expertise. For example, on March 28, 2013 we submitted our “New gTLD Security and Stability Considerations Report.” Subsequently, in May 2013 ICANN commissioned a study on naming collisions. The findings from the study, led by Interisle Consulting Group, were released on August 5. They were accompanied by an ICANN proposal, called New gTLD Collision Risk Mitigations. Both validate the reality of the risks we highlighted in March. While we strongly believe the Interisle

² See National Research Council report, “Signposts in Cyberspace: The Domain Name System and Internet Navigation.” http://www.nap.edu/catalog.php?record_id=11258

³ SAC045 - Invalid Top Level Domain Queries at the Root Level of the Domain Name System, <http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf>

⁴ SAC059 – SSAC Report on Domain Name Registration Validation - <http://www.icann.org/en/groups/ssac/documents/sac-059-en>
“CONCLUSION: The SSAC believes that the community would benefit from further inquiry into lingering issues related to expansion of the root zone as a consequence of the new gTLD program. Specifically, the SSAC recommends those issues that previous public comment periods have suggested were inadequately explored as well as issues related to cross-functional interactions of the changes brought about by root zone growth should be examined. The SSAC believes the use of experts with experience outside of the fields on which the previous studies relied would provide useful additional perspective regarding stubbornly unresolved concerns about the longer-term management of the expanded root zone and related systems.”

⁵ Letter from O. Crépin-Leblond to S. Crocker and C. Chalaby, dated June 7, 2013, <http://atlarge-lists.icann.org/pipermail/alac/attachments/20130611/2e639e17/CoverLetter-AL-ALAC-CO-0613-01-00-EN-0001.pdf>

⁶ GAC Durban Communiqué, Section IV.8, dated July 18, 2013, <http://durban47.icann.org/meetings/durban2013/presentation-gac-communique-18jul13-en.pdf>
“The GAC Shares the security and stability concerns expressed by the SSAC regarding Internal Name Certificates and Dotless Domains. The GAC requests the ICANN Board to provide a written briefing about: i. how ICANN considers this SSAC advice with a view to implementation as soon as possible. The GAC believes that all such stability and security analysis should be made publicly available prior to the delegation of new gTLDs. ii. The GAC Advises the ICANN Board to: a. As a matter of urgency consider the recommendations contained in the SSAC Report on Dotless Domains (SAC053) and Internal Name Certificates (SAC057).”

study did not go deep enough in assessing risk largely due to a late start and limits in time and resources, its conclusions echo those of Verisign's report on March 28.⁷ At that time, however, ICANN and many others were dismissive of our report and pressed forward with their announced date to recommend strings for delegation on April 23, 2013.

Even after ICANN chose to delay the April date, and with our March 28 report in-hand, ICANN continued to claim there was nothing to be concerned about with respect to the security of new gTLDs and that they were moving forward with their April target date.⁸ However, ICANN then moved its target delegation date to August, and now to September. Verisign's efforts very likely helped prevent substantial damage and disruption to users of global Internet infrastructure. It should be clear that ICANN must be more receptive to multi-stakeholder input, which will enable it to be less reactive in planning the rollout of new gTLDs.

Verisign takes all of its contractual obligations very seriously, including the two raised in your letter: to delegate new gTLDs into the root when directed by NTIA, and to serve the public interest regarding security and stability. Nothing we have said or done conflicts with the first, and we have been diligent in the second.

Therefore, if NTIA believes, as stated in your letter, that the authority to order delegations, along with the ability to order the removal of delegations together comprise

⁷ Security, Stability & Resiliency Update audiocast, ICANN Durban Meeting, dated July 17, 2013, <http://durban47.icann.org/node/39759>).

QUESTION: "There was work regarding the Public Suffix List that defines what is a varied registry in all the browsers...The problem is essentially with well-cut (phonetic) cookies, as far as I understand."

LYMAN CHAPIN (INTERISLE CONSULTING GROUP): "Right. There is a separate issue that we didn't cover in the study but is definitely of concern which is how are we going to ensure that these new domains, these new suffixes, are recognized as valid, but that was not something that we looked at in this study but is definitely something that ICANN and SSAC and a bunch of other folks are worried about."

...

QUESTION: "...Have you done any further study to determine whether or not wireless area medical networks, wireless medical devices or other extremely sensitive, very high-risk applications to the DNS may be impacted? Also, you said SIP communications are one of the series of traffic that you are seeing within your study. Have you done any study to determine whether or not any of the SIP communications may be communicating with PSAPs, public safety answering points like even 911?..."

LYMAN CHAPIN (INTERISLE CONSULTING GROUP): That's a very good point. The study gives us a lot of information about how frequently we see these things. It doesn't tell us a lot about what the consequences of name collision might be for any individual string, and I would be just as concerned as you are to make sure that before I made a judgment about the product of those two things, which is what we use to assess risk, that I did some serious investigation of what the consequences for strings like the ones you mentioned would be.

⁸ *Bloomberg BNA*, "New TLDs Security Risks Persist; Narrow Impacts Could Have Broad Ramifications," dated May 8, 2013.

sufficient controls to manage instability and security risks, and that the timeframe articulated by ICANN's senior management for the delegation of new gTLDs is appropriate, we can agree to disagree and Verisign will still act in accordance with its contractual obligations. We believe, as we are sure you do, that any such disagreement on the degree of risk does not restrict our right and obligation as an experienced operator to publicly voice our concerns. The solid working relationship that we have had over the years should continue even when we disagree on the severity of the risks and paths for risk mitigation.

Regarding the work of the Root Server System Advisory Committee (RSSAC) to which you refer, we are pleased that the RSSAC is developing instrumentation recommendations which include an early warning system. We continue to advise, however, that delegation of new root zone entries at any rate should not be permitted until these systems (which are not yet developed and for which the requirements are not yet completed) are thoroughly reviewed and robustly tested, and even then scaled at a rate commensurate with the importance of the root zone. Consistent with good security practices, these proposals, which only recently began to be discussed, should be reviewed and posted for public comment to ensure that haste has not overlooked critical requirements.

A key objective of SSAC's 2010 recommendations for early warning and root instrumentation was to provide sufficient data to ICANN to forewarn users and others of the potential impacts of new gTLDs. This pre-delegation responsibility fell squarely on ICANN. However on August 5, 2013, ICANN unilaterally and abruptly proposed to shift this obligation (to include early warning mechanisms and potentially impacted party notification) and associated liabilities, without notice, to applicants and new gTLD registry operators who are not ideally positioned to discharge these obligations. In addition, even if registries were able to fully implement ICANN's new risk notification regime, there would be little or no time left for those impacted parties to take appropriate protective measures. This transfer of risk is new and contrary to all previous recommendations that have been made by ICANN and its Advisory Committees over the last several years.⁹ We hope you will in some way address this proposed new transfer of risk to businesses and consumers by ICANN.¹⁰

The deployments of DNSSEC into the root in July 2010, and the automation of the Root Zone Management System in July 2011, are excellent examples of the collaborative success that ICANN, NTIA and Verisign have achieved together. Both of these successes, however, have had deployment paths that were well tested with agreed upon check points with vetted and measured success criteria, over extensive periods post initial deployment, with adoption and implementation of a broad set of recommendations. We would advise that the deployment of the

⁹ See recommendations 1 and 2 in SAC045 Invalid Top Level Domain Queries at the Root Level of the Domain Name System, <http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf>

¹⁰ See Letter from R. Goshorn to J. Jeffrey, dated June 14, 2013, <http://www.icann.org/en/news/correspondence/goshorn-to-jeffrey-14jun13-en.pdf>

monitoring, instrumentation and management capabilities for the root zone enjoy similar consideration, and ultimately, success.

Motivated by the presentation of name collision risks and SSR issues in Durban a few weeks ago by ICANN and their contractor, Interisle Consulting Group, our technical team endeavored to provide some additional analysis, which Interisle stated during the presentation's Q&A it did not have the data or time to conduct.^{11,12} We have submitted the methodology and findings to the SSAC and broader Internet community for review and comment, and we will post it, along with additional analysis, during ICANN's open comment period on the Interisle Consulting Group study. We also attach the report here, "New gTLD Security, Stability, Resiliency Update: Exploratory Consumer Impact Analysis," which we believe, with just a cursory exploration, clearly demonstrates the deep complexity in the interdependencies of the DNS and a number of network services and Web protocols, which have implications well beyond the matter of root zone delegations.¹³ The many resulting non-obvious but very serious risks to businesses and consumers we were able to identify and document with just a few weeks work bear careful study, and provide a new foundation for future work.

The evolution of the new gTLD program demonstrates the importance of the DNS as a critical layer of Internet infrastructure that one-third of the global population relies on hundreds of billions of times every day, and that over \$200 *billion* in e-commerce in the U.S. alone is built upon. For more than 16 years, we are proud to have operated a large part of that infrastructure

¹¹ Security, Stability & Resiliency Update audiocast, ICANN Durban Meeting, dated July 17, 2013, <http://durban47.icann.org/node/39759>

QUESTION: "...A couple questions. The first is about the dataset. The day-in-the-life data was around 48 hours. More a comment than anything else, I think it does a good job covering time of day but not really day and week, so there could be a whole host of issues that are at the periphery that we aren't seeing, whether it's on the weekend, processes that could kick off on the weekend. Just a suggestion you might want to do instead of ten terabytes, a hundred for all week or something. Thoughts?"

LYMAN CHAPIN (INTERISLE CONSULTING GROUP): "It would definitely be better if we had a dataset that spanned a much, much longer period of time, in particular one that spanned things like the first day of the week, the first day of the month, the first day of a fiscal quarter. I completely agree. We were limited to the day-in-the-life data primarily because, first of all, those are the most complete data that are readily available, and also it enabled us to do a little bit better apples-to-apples comparison because of the uniformity in the way in which that exercise is conducted. An alternative would be to do your own data-gathering exercise with the cooperation of the root server operators and so forth, but it's daunting because these datasets are huge. These files are enormous and running processing, we're using very large multi-core processors and it's still taking days to go through some of these datasets, but your suggestion is absolutely correct. A better coverage of time would give a better read on what's actually happening."

¹² A larger data set is available through DNS-OARC, and can be validated by any interested party. See <http://www.dns-oarc.net/>.

¹³ Verisign Labs Technical Report, "New gTLD Security, Stability and Resiliency Update: Exploratory Consumer Impact Analysis," <http://techreports.verisignlabs.com/tr-lookup.cgi?trid=1130008&rev=1>

August 8, 2013
Page -6-

with unparalleled reliability. Our interests are straightforward: We want that reliability to continue, which we believe is in the public interest.

Sincerely,



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



Danny McPherson
Vice President and Chief Security Officer
VeriSign, Inc.

CC: Ms. Elise Gerich, Vice President, ICANN