VERISIGN

In its March 18, 2014 FAQs on the IANA Stewardship Transition, NTIA stated, "*Aspects of the IANA functions contract are inextricably intertwined with the Verisign cooperative agreement (i.e., authoritative root zone file management), which would require that NTIA coordinate a related and parallel transition in these responsibilities.*" As this long anticipated "ramp down" of the cooperative agreement begins, we believe the CWG could benefit from a broader discussion of some of the legal, policy and operational aspects of the root management even though Verisign's role as Root Zone Maintainer (RZM) is not directly in scope for the CWG on IANA Stewardship Transition.

We have outlined below some of these broader topics for the consideration by the CWG. Verisign would be pleased to discuss these and other topics if requested.

- Some have said that any transition should yield services "at least as reliable and secure" as the services now enjoyed by the multi-stakeholder community. We think the checks and balances in the current three-party arrangement have been an important part of the success of the current system. The CWG should consider the operational capabilities of another party to stand in the shoes of NTIA and/or Verisign. The community has benefited from the operational aspect of the RZM function being performed by a public company whose shareholders have the right to elect a board of directors who appoint the Company's officers, all of whom could be personally liable for damages resulting from breaching their fiduciary duties. The CWG should explore how this creates a powerful incentive for Verisign to put policies and procedures in place to ensure operational preparedness in all operations and especially those involving the root. Public companies such as Verisign have audit committees comprised of independent directors; independent and internal auditors, and numerous other internal and external auditable processes that help ensure operational excellence by demanding management focus and oversight on operational and cyber security issues.

- The CWG should consider ICANN's operational readiness to perform or manage operational tasks associated with the root, particularly if no new external operational oversight or accountability mechanisms exist. With an understanding of the governance issues explained above, ICANN's uneven operational performance record to date could pose a substantial risk to the many billions of dollars of ecommerce and other critical functions that depend upon a stable, secure, and operational root. Poor performance of root functions could accelerate discussions already taking place about root and broader Internet fragmentation. A transition to another entity of these important functions creates risks to continuity and stability absent assurances that operational preparedness will be prioritized. ICANN, like most other network operators, has suffered service outages including a string of recent security incidents, the latest of which that were publicly disclosed include the May 2014 Registrar Database (RADAR) compromise and subsequent extended downtime, and the November - December 2014 breaches of the Central Zone Database System (CZDS), the second such security incident to impact the system this year, as well as the Governmental Advisory Committee (GAC) website that ICANN manages, the ICANN Blog, and the ICANN WHOIS Information Portal. A compromise or outage (particularly in a DNSSEC-enabled system) of the operational elements of the root zone system could have a catastrophic global economic impact and a disproportionate impact on U.S. commerce. We

believe that a multi-party arrangement with a human element in the loop for root zone changes remains imperative, irrespective of what organizations are involved.

- SSAC in SAC069 has stated that NTIA's role in administering the IANA Functions contract may be at least partly responsible for shielding ICANN from improper interference. The CWG should consider how a follow-on organization might duplicate this deterrence function now credited to the NTIA. Additionally, any role that NTIA plays in obtaining Office of Foreign Asset Control (OFAC) licenses from the U.S. Department of Treasury for root zone changes that may interfere with governmental sanctions or other restrictions should be investigated by the CWG, and accommodated as appropriate in any proposed future state.

- The CWG should understand fully the role NTIA now plays in DNSSEC and potentially other security features as they relate to the root. For example, in mid-2013, NTIA unilaterally postponed the root zone KSK rollover preparations because "the introduction of new generic top level domains (gTLDs) could be better understood with respect to their impact on the overall stability and security of the DNS before proceeding with a KSK rollover." NTIA delayed the KSK rollover to assess its potential impact on the introduction of new gTLDs. NTIA later issued a requirement for the root zone partners that these time-sensitive critical technical preparations not restart until ICANN and Verisign provide a plan that, among other things, includes express consideration of "how to avoid inadvertently prejudging or negatively impacting the ongoing multi-stakeholder efforts to develop the IANA functions stewardship transition proposal." Both the original delay for purposes of the new gTLD program, and the subsequent instruction to avoid impacting the transition, illustrate that the NTIA performs a role in this area. A fulsome discussion of this role is necessary to assure that the CWG is fully informed about the scope of the roles involved in root management, particularly those not codified in the root zone provisioning systems themselves.

- Verisign presently enjoys limited antitrust immunity as the contracted party performing the root zone management function at the direction of NTIA under the holding in *PGP Media, Inc. v. Network Solutions*. A transition of the root zone management counterparty status from NTIA may weaken such protections to Verisign or a successor organization. The CWG should discuss and consider this issue including avenues that could substitute for the immunity now enjoyed. For example, there may need to be legislation if such immunity is to be continued. In any event, the CWG should discuss the proper allocation of risk between the parties performing root zone management and the customers who presently enjoy at no cost the benefit of that work. Verisign is not and has not been compensated for the performance of the functions associated with root zone maintenance and it has never been indemnified for this work.