Verisign submits the following comments in response to the request for public comments on the DNS Risk Management Framework report from Westlake Governance posted on August 23, 2013 at http://www.icann.org/en/news/public-comment/dns-rmf-final-23aug13-en.htm.

We note the following statement made by Rick Koehler in the Initial Comment Period: "It should be clear if the framework is designed as an Enterprise Risk Management Framework for ICANN the organization or if the framework is designed as a DNS Risk Management Framework." It is our view that the framework as drafted is about risks to DNS systems and we strongly believe that the key issue ICANN should be concerned with is risks resulting *from* the DNS, without overlooking the former.

Two statements in the report make this quite clear:

- "Put another way, an event that does not affect the Availability, Consistency or Integrity (ACI) of the DNS is outside the scope of the risk management framework." (p.8)

  In other words, according to the document, if something relying on the DNS "breaks" because of actions performed by the DNS (e.g., delegation of a gTLD with name collisions), it's not a risk. As long as the DNS itself responds to requests, returns the same value everywhere in response to a request, and the value is "correct" – it doesn't matter if the value returned introduces a risk somewhere else. This is a very limited view of risk management focused only on whether the DNS is at risk – not whether everything in the Internet that relies on the DNS is.

- "SSR represents an internal view of the DNS, from the perspective of people who understand its workings and many of the threats it faces. ACI is an external view that does not require understanding of the complexity of the technology or the threats it faces, emphasizing what the DNS delivers rather than the prerequisites for its successful operation." (p.9)

  This view of SSR is totally opposite to the discussion that Verisign encourages, which is about the impact of DNS on security and stability of the Internet not just internal operations of root servers and other name servers. What the DNS "delivers" is a critical part of its systemic risk profile, and it's imperative that the implications the DNS has and the role DNS plays in the global Internet ecosystems be the foremost concern of ICANN. Due consideration for consumers and businesses that rely on the DNS, not for the sake of accessing content in the DNS itself but for enabling safe, stable, secure navigation on the Internet, must be top of mind.

A key question that the ICANN Board DNS Risk Management Framework Working Group (DNS RMF WG) and the Board itself should ask is this: Should ICANN only be accountable to

its narrow DNS operational role or to the broader Internet community that may experience the impact of DNS risks that result from actions taken by ICANN.

One other item of note regards the DNS "expert panel" and the independence of ICANN. We wholly concur with the text in the document as quoted below and believe it will be increasingly critical to the success of ICANN in the future as the multi-stakeholder model and a continually expanding business and operational role evolve:

> "To be effective, the Expert Panel must be independent of ICANN in the sense of being able to operate "without fear or favour" of management or board reactions, especially if the Expert Panel may have identified a risk that ICANN staff or managers were unwilling to address. Such unwillingness may, for example, arise because mitigation strategies could threaten achievement of managers' targets (see above – inappropriate incentives), so ICANN employees or voting board members would not be members of the Expert Panel, although members of staff would need to participate in its activities and provide it with administrative support. This Expert Panel will in effect act as ICANN's "guardians of the risk culture" in relation to the DNS."