**Comments of Ramses Martinez, Information Security Director, Verisign, Inc. on the** **Public Call by the Stability, Security, and Resilience of the DNS Review Team (SSR-RT)**

I appreciate the opportunity to provide input to the SSR-RT. Please find my comments below in *italic font* below following the text of items 4 through 7.

4. Experiences, difficulties, unexpected advantages, and lessons learned in the implementation of DNSSEC.

*Most of what Verisign encountered was around the harmonization of current standards and policies from the physical security side to suit the needs of the key management infrastructure for this system. These issues were specifically the result of the original specs for the system being incorrectly attributed the same level of security as those for the PKI environment that we previously managed.*

*Anytime authentication and integrity functions are added to an information system it becomes more brittle. As a result, operational and change management procedures associated with those systems must be adapted and become more mechanical in nature. Because DNSSEC makes the system more brittle, it requires more care and feeding, as opposed to the 'fire and forget' model that was prevalent prior to widespread DNSSEC implementation.*

5. Sources of risk analysis for the DNS, as well as contingency planning, business continuity planning (BCP) and related work for the DNS.

*Risk analysis in the information security field should be conducted as a function of the business with specific consideration given to the position in the marketplace of the particular entity for which the risk analysis is being conducted; the same is true for business contingency and continuity planning. Mature frameworks for each of these areas already exist and should be used for any entity operating in the DNS space; examples of these are COSO, NIST and ISO 27002. These frameworks are designed in an extensible and portable enough manner to be suitable for the DNS industry.*

*It would be my recommendation that consideration be given to using the aforementioned frameworks/standards rather than developing purpose-made risk analysis standards for the DNS infrastructure space.*

6. Original solutions proposed to increase the Stability, Security, and Resilience of the DNS at the protocol level, including the design of the Root Server system.

*Operational discipline would be at the top of my suggestions; most of the operational or security issues that I have seen to date are not the result of poorly written protocols or flaws in the architecture of the DNS system but rather poor implementation of the existing standards and processes.*

*Existing frameworks or standards such as ITL, COSO, NIST or ISO enable operation at peak efficiency and often result in reduced cost of operation for the infrastructure. As far as the design of the root server system goes, the current configuration enables the most reliability, security and resiliency for the global users of the Internet.*

7. Processes used by DNS users and operators to guarantee that the Risk Analysis related to the DNS is comprehensive and updated.

*I believe more education is needed about how to conduct risk analysis using the current frameworks and tools. Each entity would then have to conduct their risk analysis that captures their own risk in discrete and aggregate form and allows them to manage this risk in a manner that is viable for their particular business model.*

*Risk analysis models should explicitly recognize DNS as a critical asset that enables nearly all Internet-facing and internal transactions in today’s IP networking environments. Application of well-practiced systematic approaches to risk analysis that fully enumerates the role of the DNS in enabling user-desired or machine-initiated transactions and appropriately considers systemic elements of the DNS (e.g., registrant credentials, registrar operations, registry and managed DNS resiliency functions, recursive name servers operation) is elemental to any comprehensive risk analysis plan.*