COMMENTS BY KENYA ON THE NOTICE OF INQUIRY/REQUEST FOR COMMENTS ON THE INTERNET ASSIGNED NUMBERS AUTHORITY (IANA) FUNCTIONS BY THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE.

1. The IANA functions have been viewed historically as a set of interdependent technical functions and accordingly performed together by a single entity. In light of technology changes and market developments, should the IANA functions continue to be treated as interdependent? For example, does the coordination of the assignment of technical protocol parameters need to be done by the same entity that administers certain responsibilities associated with root zone management? Please provide specific information to support why or why not, taking into account security and stability issues.

Response 1:

All these functions should be performed by IANA we are not sure there are any advantages in separating the functions of IANA. However, we would like to propose transition over to an arrangement similar to the Affirmation of Commitments that replaced the U.S. government's MoU with ICANN.

A stronger role for ccTLDs (and through them governments) and IANA customers should provide oversight. The requirement for approval of Internet DNS root zone by the US Department of Commerce's NTIA should transition into a multi stakeholder relationship, where various stakeholders (Root Server Operators, IETF/IAB representing the protocol developers; RIRs the IP address functions, ICANN the gTLDs, ccTLDs and GAC would manage and oversee the functions.

ICANN could still host but it should be separate from the ICANN board and executive.

Further, the delegation of the IANA function should be converted from a 'Procurement Contract' to a 'Cooperation Agreement' to enhance stability in the running of the DNS.

2. The performance of the IANA functions often relies upon the policies and procedures developed by a variety of entities within the Internet technical community such as the IETF, the RIRs and ccTLD operators. Should the IANA functions contract include references to these entities, the policies they develop and instructions that the contractors follow the policies? Please provide specific information as to why or why not. If yes, please provide language you believe accurately captures these relationships.

Response 2:

Yes, the reference to these entities should be included since Internet is a multilayer, multiplayer entity. Also, reference to these entities will enhance the multi-stakeholder involvement by IANA, given that Internet has increasingly become a global facility. In particularly responding to ccTLD decisions, which in most cases, are made through national policy processes. This is also in support of the WIS Tunis agenda as well as the US Government's Principles on the Internet's Domain Name and Addressing System.

3. Cognizant of concerns previously raised by some governments and ccTLD operators and the need to ensure the stability of and security of the DNS, are there changes that could be made to how root zone management requests for ccTLDs are processed?

Response 3.1:

Yes.

Please provide specific information as to why or why not. If yes, please provide specific suggestions.

Response 3.2:

We propose transitioning out the role of the US Department of Commerce's NTIA and providing more stakeholder oversight including but not limited to the root zone changes. The process needs to be automated, with IANA receiving, validating and authorizing root zone change requests without reference to the NTIA.

4. Broad performance metrics and reporting are currently required under the contract.\7\ Are the current metrics and reporting requirements sufficient? Please provide specific information as to why or why not. If not, what specific changes should be made?

Response 4:

Performance should be subjected to review and monitoring mechanisms similar to those under the Affirmation of Commitments (AoC) for ICANN. Further, IANA should develop Service Level Agreement for its root zone management function in collaboration with the ccTLD community. This SLA should include detailed documentation in all UN languages on root zone management functions as well as provide a clear framework for delegation and redelegation. IANA should receive, validate and implement any Internet DNS root zone requests without reference to the NTIA.

5. Can process improvements or performance enhancements be made to the IANA functions contract to better reflect the needs of users of the IANA functions to improve the overall customer experience? Should mechanisms be employed to provide formalized user input and/or feedback, outreach and coordination with the users of the IANA functions? Is additional information related to the performance and administration of the IANA functions needed in the interest of more transparency? Please provide specific information as to why or why not.

Response 5:

IANA should introduce a member or user-only area only through login that makes it easy for users to submit requests. The processes in the current IANA contract has been and still seem adequate, however, regular request for comments from the Internet community on process improvement and performance enhancement would be both insightful and useful.

Further, involvement of the various Internet stakeholders in reviewing and monitoring the IANA and related processes, as is in the case of ICANN's Affirmation of Commitments (AoC), would enhance confidence in the its functions and help create a more transparent process.

6. Should additional security considerations and/or enhancements be factored into requirements for the performance of the IANA functions? Please provide specific information as to why or why not. If additional security considerations should be included, please provide specific suggestions.

Response 6:

IANA should continue to enhance security on the DNS Root. The current security considerations seem adequate and the implementation of eIANA is expected to increase the level of security. However, security considerations should be reviewed regularly, to ensure that the security measures remain current can use commonly available tools for signing and validation of signatures and are in line with the global network and information security best practices and standards.