Thursday, March 31, 2011

Fiona M. Alexander
Associate Administrator
Office of International Affairs
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4701
Washington, DC 20230
IANAFunctions@ntia.doc.gov

Re: Call for Comments on Internet Assigned Numbers Authority (IANA) Function

Originally published in the Federal Register/Vol. 76, No. 38/Friday, 2011 / Notices, pages 10569 to 10571.[1]

Prefatory Remarks: We are grateful that the NTIA has undertaken a comprehensive review of the IANA Functions contract, the first since the expiry of the DARPA/USC contract.

As several of the questions address the issues of performance and entities within the Internet technical community we wish to declare that one of the authors of this comment was retained by the IANA in 2007 to implement the ICANN / IANA - IETF MoU Supplemental Agreement,[2] and this informs our comments which relate to the issues of performance and entities within the Internet technical community.

As the set of functions referred to as "the IANA function" are actually four distinct sets of functions, our response to Question 1 is unfortunately lengthy, setting up the context for our responses to Questions 2 through 6.

Additionally, while the six set questions address important issues, they do not exhaust the scope of a comprehensive review, and after offering our responses to these questions we briefly address some additional topics.

Response to Question 1: Should the IANA functions continue to be treated as interdependent?

There is no technical or institutional necessity to treat the IANA functions as interdependent.

---

[1] http://www.ntia.doc.gov/frnotices/2011/fr_ianafunctionsnoi_02252011.pdf
[2] http://www.icann.org/en/general/ietf-iana-agreement-v8.htm

Writing for the Internet Architecture Board, editors Danny McPherson, Olaf M. Kolkman, John Klensin and Geoff Huston point out in Defining the Role and Function of IETF Protocol Parameter Registry Operators[3] that the set of functions defined in the Supplemental Agreement may be implemented by one or more distinct operators, consistent with the direct experience of one of our authors as the implementer of the reporting function which has informed the IETF since May, 2007.

In our view the question is in two parts. First, a review of the candidate operators of the protocol parameter registries, and second, an examination of actual, or latent adverse consequences from any possible operator selection.

Several candidate operators of the protocol parameter registries come to mind. The IETF and ISOC are, as Bill Manning notes in his comment,[4] significantly more institutionally capable today than they were in 2000. Several academic institutions, Berkeley, Carnegie Mellon, and Harvard to name just three, are also capable of carrying out the operator responsibilities. Finally, as ICANN's current executive, Rod Beckstrom observes in ICANN's comments (14 pp, .pdf),[5] ICANN is capable of carrying out the operator responsibilities. Thus, there are several functionally equivalent choices available to the Department to solicit contracted operations of some or all of the protocol parameter registries operations portion of the IANA functions, at least two of which have an existing institutional responsibility, and independent means, to conduct those operations.

The possibility of latent adverse consequences is unfortunately presented in the conceptualization of the protocol parameter registries as something which should be privatized, or for that matter, something functionally affected one way or another by the corporate form of one or more of the registries operators. As an abstract question we can find no rational basis to support a claim that the IANA function must be, or ought to be, carried out by a private or public entity, or a basis to distinguish between private entities, e.g., Verisign and ISOC, or public entities, e.g., between NIST and GOST.

In this we differ from Rod Beckstrom's statement of ICANN's position on the subject, which unfortunately construes the operations of the protocol parameter registries created by the IETF as functions the White Paper committed the United States Government to both obtain exclusive control over, and subsequently transfer as an asset to a single private actor.

We observe that the existence of an IANA Considerations section in an Internet Draft does not create a government interest in, or title to, a protocol parameter. See IETF Trust Legal Provisions (TLP) Documents[6] and RFC 5378 Rights Contributors Provide to the

---

[3] http://tools.ietf.org/html/draft-iab-iana-07
[4] http://www.ntia.doc.gov/comments/110207099-1099-01/comment.cfm?e=8B430831-4634-4A6B-845B-97673CD97842
[5] http://www.ntia.doc.gov/comments/110207099-1099-01/comment.cfm?e=273CB4D8-1EF6-4172-B96E-EF609E04F8BE
[6] http://trustee.ietf.org/license-info/

IETF Trust (BCP 78)[7] and RFC 3979 Intellectual Property Rights in IETF Technology, and RFC 4879 Clarification of the Third Party Disclosure Procedure in RFC 3979 (BCP 79),[8] as well as RFC 5377 Advice to the Trustees of the IETF Trust on Rights to Be Granted in IETF Documents.[9]

No security and stability issues arise from the routine process of accepting Internet Drafts for publication, update, last call, or evaluation, or for the issuance of MIME media types, port assignments or modifications, Telephone Routing over IP (TRIP) parameters, multicast assignments or all other protocol parameters.

The Numbers Resource Organization has not provided guidance, as the Internet Architecture Board has, however those functions which relate to number resources may reasonably be undertaken by the NRO, for reasons that are mentioned in the response to Question 2.

We wish to point out an apparently overlooked security and stability issue relating to prefixes and Autonomous System Numbers.

The Border Gateway Protocol (BGP) is currently the only Internet routing protocol used to maintain connectivity between autonomous systems. BGP is a path vector protocol where each router selects best routes to destinations based on the routes advertised by neighboring routers.

Published measurements of routing changes in the Internet have shown that there can be considerable delay in BGP convergence. These studies also observed that high levels of route fluctuation during delayed convergence have an adverse effect on end-to-end traffic delay, resulting in packet loss and intermittent disruption of connectivity.

Administrative acts may intentionally induce a repeating cycle of sending and receiving prefix updates and/or withdraws. This was observed to occur on January 27th and February 2nd, 2011, and again on February 18th through March 5th, 2011. These administrative acts were insufficiently frequent to cause churn in the Default Free Zone, or affect global end-to-end traffic, outside of the withdrawn prefixes. However, these acts were unremarked upon in their substance, and no guidance was offered the administrations responsible, or administrations informed by the Internet technical community, that the global routing system was not designed to accommodate arbitrary announcements made for the purposes of reducing regional routes in the global routing table.

While no security and stability issues arise from the routine process of accepting applications for prefixes and autonomous system numbers, an awareness of intentional capabilities to cause pathological outcomes is desirable in the designated operator of the functions which relate to number resources.

---

[7] http://tools.ietf.org/html/bcp78
[8] http://tools.ietf.org/html/bcp79
[9] http://datatracker.ietf.org/doc/rfc5377/

The IANA root zone file editor function, which we point out in passing, ensures the existence of the .arpa, .edu, .gov, .int, .mil, and .us zones and their respective delegations and thereby provides a direct benefit to the Federal Government of the United States of America, has not been the subject of a memo similar to the IAB's memo on protocol parameters and their registries, summarizing current operational requirements and and clarifying issues that have arisen since any prior summary of record, with the notable exception of the operational deployment of DNSSEC.

As in our response to the first part of this question, concerning the protocol parameter registries, in our view the question is in two parts. First, a review of the candidate operators of the IANA root zone file editor function, and second, an examination of actual, or latent adverse consequences from any possible editor selection.

Several candidate editors of the IANA zone file come to mind. ISOC is again a reasonable candidate, as is OARC and ICANN (which currently makes recommended edit changes) and Verisign (which actually executes the edit function). Thus, there are several functionally equivalent choices available to the Department to solicit contracted operations of the IANA root zone editor function, at least two of which have an existing institutional responsibility, and independent means, to conduct those operations.

The possibility of latent adverse consequences is unfortunately presented in the conceptualization of the IANA root zone editor function as primarily a political, rather than a technical activity, and one in which the United States Government has no direct beneficiary interest. A further latent adverse consequence is also unfortunately presented in the conceptualization of the IANA root zone editor function as bound inexorably to the newly introduced operational practice of signing zones (DNSSEC), etc. There is too the unfortunate period of record, mentioned in our response to Question 2.

Finally, there are the functions of operating the .int and .arpa top-level domain registries, and the operations of the "L" root server. Our concerns are offered within the body of our response to Question 6, infra. We point out in passing that only the "I", "K" and "M" instances of the IANA root server constellation are located outside the jurisdiction of the United States, and that the distribution of jurisdictionally distinct servers of the IANA root has made no progress in the past eleven years.

Several candidate operators of the .int and .arpa top-level domain registries come to mind, those mentioned above as candidates for other functions currently carried out by the IANA, as well as among the top-level domain registry operations community.

Response to Question 2: Should the IANA functions contract include references to [the IETF, the RIRs, the ccTLD operators], the policies they develop and instructions that the contractor follow the policies?

For those functions described by McPherson et al, supra (the IETF protocol parameter registries), a normative reference would be superfluous.

For those functions which relate to number resources, and we point in passing that the primary allocation responsibility, documented in RFC 1466[10] passed from the IANA function to the RIRs seven years before the publication of the White Paper, we also think a normative reference would be superfluous.

While the inclusion of normative references in contract(s) for the above set of functions is not warranted, it is advisable -- and fair -- to recognize, in more general terms, the role and contribution of those technical bodies, e.g., in an informational section of those document(s).

For those functions which relate to the root zone editor function, given the unfortunate period in which those functions were administratively degraded, we think it prudent that contracts which include performance of those IANA functions contain explicit references to the ccTLD operators and the policies they develop, as well as instructions to the effect that the contractor(s) must follow those policies.

Draft language we believe accurately captures this specific relationship may be of the form "Policies developed by the ccTLD operators, through the ccNSO or other means, shall be binding upon the root zone file editor." We think that this or a similar statement of obligation, if present during the third week of March, 2010, would have resulted in an improved initial response to the introduction of the .C variant of the Conficker distributed system, and would have resulted in an improved long-term plan and response to the .C variant, and prevented the externalization of .C interposition cost to the ccTLD operators.

Response to Question 3: Are there changes that could be made to how the root zone management for ccTLDs are processed?

In our view this is not one question but several.

There is a class of change requests for which the processing is conditional, e.g., redelegation requests arising from attempts to correct the capture of delegations from late adopter states by private, usually foreign domiciled for-profit entities. This class is unfortunately not small, but it does not give rise to stability and security concerns. Never the less, the privatization-by-capture of delegations, primarily to weak Pacific Island and African territories, is a problem, and change requests to the root zone by captured operators is an area where policy needs to be developed.

There is a class, fortunately quite small, for which the processing has given rise to stability and security concerns. We must point out that a redelegation within the course of belligerency has had the profoundly unfortunate, and we hope temporary, effect of making the DNS a target for state and non-state actors, using conventional or

---

[10] http://tools.ietf.org/html/rfc1466

computational forces. While the 2005 redelegation of .iq may not be a curable error at this point in time, changes to the root zone management processing should ensure that redelegation by force is much more difficult, if not impossible.

Finally, there is a class of requests which has, up until 2010, been deferred, which has given rise to a distinct, but serious concern. With the introduction and delegation of labels in scripts other than Latin, this concern is greatly reduced, but not completely eliminated. In our view, management of the root causes for non-uniqueness in the global DNS is of the highest importance, consistent with the IAB Technical Comment on the Unique DNS Root.[11]

Response to Question 4: Are the current metrics and reporting requirements sufficient?

For those functions described by McPherson et al, supra (the IETF protocol parameter registries), as implemented by an author of this comment, our answer is in the affirmative.

For those functions which relate to number resources, again, our answer is in the affirmative, though again we note in passing that most any metric and reporting requirement became superfluous after the publication of RFC 1466.

For those functions which relate to the root zone editor function the current metrics and reporting requirements are not sufficient, as they do not anticipate the operational issues introduced by signing the IANA root zone and key management issues which are still being explored in the first large scale operational application of zone signing. This is an area where NIST can, and in our view, should, lead in the ongoing development of metrics and reporting requirements.

Response to Question 5: (a) Should mechanisms be employed to provide formalized user input and/or feedback, outreach and coordination with the users of the IANA functions? (b) Is additional information related to the performance and administration of the IANA functions needed in the interest of more transparency?

We see no compelling utility or necessity at present for formalized user input and/or feedback, outreach and coordination with the users of, or additional information related to the performance and administration about, the IANA functions.

Response to Question 6: Should additional security considerations and/or enhancements be factored into the requirements for the performance of the IANA functions?

For those functions described by McPherson et al, supra (the IETF protocol parameter registries), and for those which relate to number resources, such security considerations

---

[11] http://datatracker.ietf.org/doc/rfc2826/

and/or enhancements would be superfluous. For those functions which relate to the zone editor function, experiencing the first large scale operational application of zone signing, "security considerations and/or enhancements" should not be created before the operational risks and rewards are well understood. This is an area where NIST can, and in our view, should, lead in the ongoing development of security considerations and/or enhancements.

Finally, for the function of operating the .arpa and .int registries, and the L root server, we point out that present and continuous capability is more important than requirements to meet hypothetical, or long-term needs. Top level domain registry operations is not one of ICANN's core capabilities, nor one of ICANN's core missions, and the fundamental requirement is core competency by a top-level domain registry operator, as shown by ICANN's detailed criteria for top-level domain registry operators, in particular questions 23 to 44, and several of questions 45 to 50. When an operator has been selected which meets this fundamental criteria, and NIST, together with the Internet technical community, have issued additional security considerations and/or enhancements, then these should be factored into the requirements for these particular functions and reflected in modifications to their respective contracts.

Additional Unsolicited Comments

In the view of Professor Michael Froomkin, ICANN exercises delegated rule making authority, and is properly subject to the requirements of the Administrative Procedure Act (APA), Pub.L. 79-404, 60 Stat. 237. From this the requirements for notice, transparency and accountability follow. See WRONG TURN IN CYBERSPACE: USING ICANN TO ROUTE AROUND THE APA AND THE CONSTITUTION (168pp .pdf).[12]

We do not share the view that the principles of transparency and accountability are absent in the expiring contract.

Concluding Remarks

We are broadly in agreement with the comments already submitted to the NTIA by Bill Manning and Dimtry Burkov, and we greatly appreciate the opportunity to contribute, via comments to NIST, to the first comprehensive review of the IANA Functions contract since the expiry of the DARPA/USC contract on January 1st, 1999.

Eric Brunner-Williams
ebw@abenaki.wabanaki.net

Jean-Jacques Subrenat
jjs.global@gmail.com

---

[12] osaka.law.miami.edu/~froomkin/articles/icann.pdf

Beau Brendler
beaubrendler@earthlink.net