I.   Potential list of topics that might be considered as part of RZERC's scope:

1. **Introduction of RRTYPEs not previously included in the root zone (this would cover DNSSEC in the past). (Howard)**

2. **Changes which would cause a "significant" change in size to the root zone (Significant TBD). (Howard)**

3. **Significant changes to the operation of the root zone, such as**
   - **Change in root zone operator**
     - Comments: What do we envisage RZERC's role is in this scenario? (Kim)
     - Response: Perhaps a review of any new potential operator's history as it pertains to DNS operations? Impact study of how the new operator's network coverage could potentially change query paths? (Howard)
     - Response: I suspect it is important to keep RZERC out of making judgment calls on specific vendors. I would foresee any such evaluation would be rather along the lines of reviewing the criteria against which a potential operator would be assessed. (Kim)

   - **Change in DNSSEC key algorithm or size**
   - **KSK roll?**

     - Comment: Assuming this KSK roll concludes in a normal fashion, it seems to me performing a key rollover will become perfunctory (i.e. rolling every x years). I don't see a KSK roll being elevated to this group unless it meets the other criteria above (i.e. new algorithm, possibly new size.) (Kim)
     - Response: +1 (Jim)
     - Response: What about emergency KSK rolls? I'm not saying we bless a roll before it occurs, but should we look at the procedures for this type of activity to ensure they are in line with keeping the stability of the root zone? (Howard)
     - Response: A KSK roll is probably out of scope though -- it should be a routine if infrequent event -- unless it involves a change of algorithm or key length. (Jim)

4. **Changes in operational policy (Howard)**
   - **Significant change in root DPS (Significant TBD)**

5. **Getting a root key repository outside the USA. Suppose US airspace gets closed down. Or immigration policies make it impractical for foreigners to serve as TCRs.**

- ○ Comment: What would be the scope of RZERC's consideration of such a change? Where the root management partners keep their physical facilities seems to me beyond "architectural changes to the content of the DNS root zone" (Kim).
- ○ Comment: I'm concerned that this moves us more into Layer 9 - are we going to look into International policy changes? (Howard)
- ○ Response: See above. If changes to the technical check criteria (say) are to be in scope Kim, so should a change to the location(s) of the root's KSK repository. And for the same sorts of reasons: ie some sort of notionally independent third party sanity check. (Jim)
- ○ Response: Agreed. (Kim)

II. Potential list of topics that might NOT be considered as part of RZERC's scope:

1. **Daily "standard" changes to the root zone (Standard TBD). (Howard)**
2. **Introduction of new TLDs into the root zone (subject to the size bullet above). (Howard)**
   - ○ Comment: A couple of other scenarios I had in mind that don't reflect architectural changes to the root zone content itself (Kim)

3. **Support for additional algorithms and digest types for delegations. (Kim)**
   - ○ Comment: I believe I mentioned this above for the root zone, but yes, the same could be said for delegations. (Howard)
   - ○ Comment: I think that should be considered routine operational detail rather than a major architectural change. Unless of course those new algorithms and digest types are not supported by an RFC. (Jim)

4. **Upgrades to the software used to manage the root zone and root zone workflow (except as it pertains to other characteristics deemed to be in-scope) (Kim)**
   - ○ Comment: Not sure I want to do work every time there's a patch to an operator's software. Would that also include network gear upgrades? This seems intractable to me. (Howard)

5. **Revisions to the technical check criteria for the root zone. (Kim)**
   - ○ Comment: +1. (Howard)

6. **Revisions to the authentication mechanisms for TLD managers. (Kim)**
   - ○ Comment: Not sure exactly what you mean on this last one. (Howard)
   - ○ Response: To be a little more concrete of one scenario I have in mind: I have been discussing with TLD managers a new authorization model for root zone maintenance that includes a number of facets. At the high level,

we are planning to add a new "authorizer" contact type, of which there can be any number 1..n defined, that approves change requests on behalf of the TLD operator. This replaces the current approach where the technical and admin contact for a domain are also mandatorily the co-authorizers for changes to that domain. The existing technical and administrative contacts would become WHOIS-only contacts designed for customer service purposes only. These authorizer contacts would have some new capabilities that do not exist today, such as the ability to enable two factor authentication, as well as providing the capability to configure certain authorizers to only be permitted to approve certain types of change requests, all at the TLD managers discretion. (Kim)

○ Comment: Ditto. Though I appreciate IANA might well appreciate having RZERC approve/review these sorts of changes to existing processes. Assuming there's no other appropriate third party which could do that. (Jim)

III. Other Points:

★ I assume that RZERC is not going to do any work on whatever ends up on the list we compile. Until of course someone approaches us with a proposal that's in scope for RZERC.(Howard)

○ Comment: I think that's correct. What we discussed on the call was having illustrative scenarios that would inform thinking about what is in-scope and out-of-scope. (Kim)
○ Comment: +1 (Howard)
○ Response: OK. I wonder though if we need to think much about this. (Jim)
○ Responde: An illustrative list of what is and isn't in scope has the potential to take on a life of its own. Or be seen by others to be a definitive list that lives forever and can never be changed. We should be very careful about that. Particularly once the current RZERC membership has moved on and the institutional memories we have today have either been forgotten or mutated tomorrow. (Kim)

★ An illustrative list of what is and isn't in scope has the potential to take on a life of its own. Or be seen by others to be a definitive list that lives forever and can never be changed. We should be very careful about that. Particularly once the current RZERC membership has moved on and the institutional memories we have today have either been forgotten or mutated tomorrow.(Jim)

★ Straw man suggestion: how about expecting anyone who asks RZERC to do any work provides a justification of why their proposal is in scope? (Jim)
  - ○ Comment: So I think this scoping exercise is valuable because I expect that my team will be the primary instigator of issues that will be brought to the RZERC, and *my concern is we will go along a path of implementing a change only to find out too late that RZERC felt it was obligated to go through them first*. By getting a good sense of roughly where everyone's opinions lay, it will give us some confidence as to what issues clearly need to come here, clearly do not need to come here, and those that are on-the-fence which we'll likely to flag early on and get a read on whether we need to factor RZERC consideration into our planning. It could be we are all well aligned, but hypothesizing now will hopefully illuminate areas where members feel differently in order to avoid issues in the future.(Kim)
  - ○ Response: True. Though it's usually easier to ask for forgiveness rather than permission. :-) (Jim)
  - ○ Comment: One possibility here could be for IANA/PTI to say to RZERC "We plan to do foo. Got anything to say about that before we start?". (Jim)

List of potential Root Zone topics that might come RZERC's way

Below is a list of topics related to the root zone. Some of these are events or changes that have already happened, or will happen. Some are based on active discussions within various groups (ICANN/RSSAC/SSAC, IETF/DNSOP, etc).

As an internal exercise for RZERC, we can consider whether or not these topics are within our charter. That is, if some group comes to us and says "I think RZERC needs to consider how X will affect the operation of the root zone", how would we respond?

1. Introduction of a new root zone RR type.

2. Changes to root zone TTLs.

3. Another thousand TLDs.

4. Change in DNSSEC key size for the KSK.

5. Change in DNSSEC key size for the ZSK.

6. Change in DNSSEC algorithm.

7. Change in other DNSSEC parameters (signature validity, NSEC/NSEC3).

8. Change in supported algorithms and digest types for DS records.

9. KSK rollover (assume RZERC existed 2+ years ago).

10. Geographical location of Key Management Facilities.

11. Label generation rules and use of non-ascii characters.

12. Removal of an existing RSO.

13. Addition of a new RSO.

14. Change in "ownership" of an RSO.

15. Location of root server instances.

16. Prolonged inability of an RSO to meet service level expectations.

17. Change to the naming scheme of root servers.

18. Change in DNSSEC status or parameters of root-servers.net zone.

19. Change in frequency of publishing the root zone.

20. Latency in root zone distribution.

21. Transport protocols supported by root servers (UDP, TCP, TLS, DTLS, QUIC).

22. Services provided by root servers (DNS query, AXFR)

23. Configuration of root servers with respect to MTU, MSS, fragmentation, and truncation.

24. "Significant" changes to KSK operator DPS

25. "Significant" changes to ZSK operator DPS

26. Revisions to PTI's authentication mechanisms for TLD managers.

27. Changes to technical checks performed by PTI.

28. Changes in technical checks performed by RZM.

29. Upgrades to the software used to manage the root zone and root zone workflow.

30. Applications for RFC 6761 Special Use TLDs (.onion, .local).

31. Proposal to serve root zone from (many) CPE devices.

32. Review of RZM transition plan

33. RZM transition

34. Zones, other than root, served by root servers (arpa, root-servers.net)

35. Design of distribution system between RZM and RSOs

36. Change in root zone SOA serial format (e.g. YYYYMMDDnn to epoch)

For reference, some relevant text from RZERC's charter:

I. Background

> Per the NTIA IANA Functions Contract that existed prior to the IANA stewardship transition, NTIA approval was required for the implementation of all changes to the DNS root zone environment such as the DNSSEC-signing of the root zone, many classes of changes to IANA processes, as well as edits that would be applied by the Root Zone Maintainer to the DNS root zone. Post transition, the CWG-Stewardship recommended that approval of routine content changes to the DNS root zone would no longer be required, however due to the critical nature of the root of the DNS, major architectural

==changes== would require formal approvals. The CWG-Stewardship recommended that the ICANN Board seek recommendations from a standing committee regarding the advisability of moving forward with such architectural changes. As part of implementation planning, ICANN named this Committee Root Zone Evolution Review Committee (RZERC).

II. Purpose

The Committee is expected to review ==proposed architectural changes== to the content of the DNS root zone, the systems including both hardware and software components used in executing changes to the DNS root zone, and the mechanisms used for distribution of the DNS root zone. The Committee shall, as determined necessary by its membership, make recommendations related to those changes for consideration by the ICANN Board.

III. Scope of Responsibilities

The Committee will consider ==issues raised== to the Committee by any of its members, PTI staff, or by the Customer Standing Committee (CSC) to identify any ==potential evolutionary improvements== and/or ==security, stability or resiliency risks== to the architecture and operation of the DNS root zone.

The Committee will not necessarily be the group that considers the details of the issue(s) raised, but will be responsible for ensuring that those involved in the recommendation(s) to the ICANN Board include all relevant and impacted bodies and will have access to necessary expertise to provide the best possible recommendation(s). The Committee will coordinate with the committee's respective organizations and communities, and as appropriate, external experts, to ensure that relevant bodies and impacted parties were involved in discussion and recommendation development.

For architectural changes that impose potential risk to the security, stability, or resiliency of the content of the DNS root zone, the systems including both hardware and software components used in executing changes to the DNS root zone, or the mechanisms used for the distribution of the DNS root zone (as identified by one or more committee members and agreed by a simple majority of members), the Committee will coordinate a public consultation process via the ICANN public comment forum regarding the proposed changes, including the identified risks.