# Comment on Root Zone Update Process Study

Steve Crocker, 10 April 2022



## 1. Introduction

The Root Zone Update Process Study was released for public comment on 14 March 2022. Comments are due by 25 April 2022.

I have followed the root zone update process for approximately 20 years. This is a nice piece of work. It covers a lot of ground. It is a very positive report, finding no big problems and offering a few specific recommendations for further improvement. I agree IANA does an excellent job. That said, there are areas that can be improved.

Some of my comments below address the report; others go beyond the report and address the root zone update process.

## 2. Introductory Material

### 2.1. Description of the IANA Process

It would be helpful to have a section that introduces the IANA operation and the Root Zone Update Process. This would provide a place to define the terms and concepts used in the rest of the report and to provide a bit of the history.

The description of the IANA process in the RFP states, "the IANA organization:

> Coordinates the allocation and assignment of the four sets of unique identifiers for the Internet, which are:
>
> a. Domain names (forming a system referred to as the Domain Name System, or DNS);
>
> b. Internet Protocol (IP) addresses;
>
> c. Autonomous System (AS) numbers; and
>
> d. Protocol port and parameter numbers."

It is worth including this top-level view of the IANA functions and the communities served. In the discussion of IANA staffing on p 45 and following, it would be worth noting that the protocol parameter and port registries constitute a large fraction of the workload.

Regarding history, PTI was created in 2016 as part of the Transition. What is the role of PTI management compared to ICANN management? There are references to the PTI board vs. the ICANN board. References to ICANN, IANA, PTI, and IFO are uneven.

With respect to the root zone database, each TLD has both DNS records in the root zone and contact data. The contact includes the official operator of the TLD and both admin and tech contacts. A deficiency endemic throughout the entire DNS registration ecosystem is the lack of definition of the authority and responsibility of each of these roles.

**Recommendation:** The authority and responsibility of each defined role should be documented explicitly, perhaps in the form of Table 1.

| Role | Authority | Responsibility |
|---|---|---|
| TLD Operator | *What is the TLD operator authorized to do?* | *What is the TLD operator required to do?* |
| Admin | *What is the Admin authorized to do?* | *What is the Admin required to do?* |
| Tech | *What is the Tech authorized to do?* | *What is the Tech required to do?* |

*Table 1: Authority and Responsibility for each defined role*

## 2.2. Ultra-conservative execution

A central fact about the root zone update process is that the consequences associated with executing an incorrect request are far worse than those associated with failing to execute a correct request.[1] An incorrect change to the root zone can lead to disruption of service for the entire top-level domain. Failure to implement a correct request, on the other hand, is simply a delay. The same request can be submitted again. The expected time of most changes is lengthy and imprecise, so a failure to execute a change followed by a repeated attempt may not seem different from the normal variations in the update process.

The IANA function ethic is therefore ultra-conservative. This applies to both the technical systems used and the procedures. The same ethic is echoed in the letter from Verisign,[2] which uses the phrase *"unnaturally perfect"* to emphasize the focus on avoiding errors.

# 3. Major Action Items

## 3.1. Saturday Night Massacre

"What would happen if the U.S. Government took [our] ccTLD out of the root zone." Officials of various countries have posed this question more than once. Explanations of the multiple technical and procedural checks, oversight of the personnel, etc., don't carry much weight. The imagined scenario behind this question is the full weight of the U.S. Government might be applied to force an abrupt change to the root zone, contravening all policy, procedural and technical controls. In the sequence of events referred to as the Saturday Night Massacre, a few key senior government officials refused direct orders from the President of the United States. [3] It is not hard to imagine a similar order but with a different outcome.

A closely related scenario is included in the recent request from Ukraine to remove Russia's domains from the root. ICANN refused the request. [Ukraine]

The taxonomy on pages 28-29 includes a variety of possible attacks but does not appear to cover the potential of a forceful government intervention. Possible improvements in the overall process include the use of tamper-proof hardware and/or distribution of the IANA function across multiple national jurisdictions.

Irrespective of the actual likelihood of a Saturday Night Massacre scenario, the credibility of the root zone update process would improve if ICANN could show this scenario could not succeed.

**Recommendation:** Initiate a study on how to fortify the root zone update process against an abrupt, forceful, out of policy change to the root zone.

---

[1] These are often referred to as false positive vs false negative or type I vs type II errors. See https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_positive_error

[2] [Study] pp 108-113

[3] https://en.wikipedia.org/wiki/Saturday_Night_Massacre

## 3.2. Name Servers and Glue Records

When a name server used by a TLD appears in the root zone, the address of the name server is usually required. These are referred to as "glue records."

Name servers are occasionally moved from one address to another, i.e., the name server is "renumbered." Renumbering requires coordinating multiple changes involving the TLD operators, the name server operator, and IANA.

If the name server provides service to more than one TLD, the coordination process is a bit tangled. Long-standing IANA policy has required explicit, affirmative approval from both the Admin and Tech contacts associated with **each and every** TLD. As noted in the text quoted below, the coordination is sometimes problematic and results in lengthy delays.[4]

> This sub-process confirms the identity of the requestor and ensures that cognizant TLD personnel authorized the requested change(s).
>
> This sub-process addresses several different scenarios:
>
> - If the request is for a change of Admin or Tech Contacts, then the old and new contacts must verify the change.
> - If the change request is for a nameserver change and involves a provider that serves a number of TLDs, then contacts must be confirmed for all the TLDs using that same nameserver (also known as a "glue" request).
> - Where Admin and Tech Contacts are not reachable, IANA uses either private emails, contacts through personal knowledge of the operation, or the publicly available contact of the Registry Operator / TLD Manager.
>
> These scenarios gave rise to a set of questions from IANA customers and our team:
>
> 1. Are there any exceptions to confirming either both contacts or confirming through an TLD Manager?
>
>    There are rare exceptions made with unusual circumstances that are handled on a case-by-case basis. While we prefer completely documented processes, in these difficult-to-anticipate cases, a final decision should be left to an authorised IANA team member. In such a case, the process documentation should indicate the team members that are authorised to approve these "out of band" contact confirmations.
>
> 2. What are criteria for approval based on contact with a TLD Manager?
>
>    These are generally based upon the personal knowledge, industry experience, and acumen of the IANA staff. It is difficult to document the criteria for making these calls so the process documentation should include a list of authorized

[4] [Study] pp 21-22.

personal for these out-of-band authorizations, either by name or title.

3. Requiring all "glue" contacts to agree extends the time of or bars the change. Is there a more efficient method?

   Yes. IANA staff have already been collaborating with the community to enact a change in the standard for authorising a glue change. After years of processing glue changes, it has been recognised that these changes result in improved (i.e., more stable, secure) operations and there is little or no downside risk to approving them, even in the case of one or more parties not explicitly approving the change. IANA is planning to recommend a change to the processing of glue requests from "opt-in" to "opt-out" so that, after the requestor and one other TLD has explicitly approved the change, any TLD that does not object will be presumed to have approved the change. IANA is planning appropriate community discussion and safeguards in implementing the change.

This is a very long-standing problem and has been addressed in the past. It should have been put to rest quite a while ago. See, for example, the 2009 report, [Glue], for a very readable description and analysis of the problem.

The long-standing IANA policy is based on the laudable intention of making sure all TLD operators are informed and prepared for the change.

The improvement suggested by IANA in response to question 3 in **Error! Reference source not found.** is pragmatic but fundamentally weak. As noted in [Glue] section 2.5, "the only party that is in a position to notify the TLDs of a renumbering in a timely and reliable manner is the server operator, and therefore the duty to do so should fall on the server operator, not on IANA."

One part of the coordination is IANA's rule that changes to the root zone must be requested by a TLD operator and **that only TLD operators are permitted to interact with IANA**. If IANA were able to interact with the name server operators, the coordination process could be more efficient. To go a step further, IANA could require each name server operator to enter into an agreement with IANA that sets standards for TLD name server operation and coordination of changes. Whether this suggestion would be qualitatively better than the current muddled process requires broad consultation and analysis, so this specific idea is not included here as a recommendation. However, what does seem clear is the issue of glue record coordination deserves attention. There are technical issues as well as process issues involved. The Root Zone Evolution Review Committee (RZERC) was created precisely to deal with such matters.

**Recommendation:** The RZERC should be invoked to study glue record coordination and recommend improvements.

## 3.3. Unaddressed Areas

The following topics are not addressed in the Study but are logically closely related.

### 3.3.1. Root Server Operators

The root server operators are missing from this report. The RFP scope, copied below, focuses on TLDs and excludes the actions of the Root Server Operators. However, the Root Server Operators have entries in the root zone and thus also depend on the root zone update process. Moreover, there have been instances in the past involving the introduction of AAAA records for root servers and the introduction of DNSSEC that affected the root operations and that required changes in the IANA update process.

> The scope of the study includes:[5]
>
> - The process and means by which a TLD manager submits a root zone change request to the IFO
> - All policies in place, tasks performed, and systems used by the IFO to evaluate and process a requested root zone change, from receipt of the request from the TLD manager through the means and mechanism by which the change request is communicated to the Root Zone Maintainer
> - All communications between the IFO and Root Zone Maintainer
> - All policies in place, tasks performed, and systems used by the Root Zone Maintainer to evaluate and process a requested root zone change, from receipt of the request from the IFO through the means and mechanism by which the signed root zone is distributed to the Root Server Operators
>
> To summarize, the scope begins with a TLD manager's request for a change and ends with the publication of a new root zone on the Root Zone Maintainer's platform for distributing the root zone to the Root Server Operators (RSOs). The actions of the RSOs are not in scope, except to the extent that any possible issues with the design or operation of the Root Zone Maintainer's root zone distribution platform might affect the RSOs' ability to receive an updated version of the root zone in a timely and accurate manner.

**Recommendation:** The Root Server Operators should be surveyed.

[5] [RFP] p 3.

### 3.3.2. DNSSEC

The Study explicitly excludes "any systems or processes surrounding DNSSEC signing of the root or any processes or procedures involving DNSSEC aside from the routine process of TLD managers submitting DNSSEC-related records to IANA for inclusion in the root."[6]

**Recommendation:** A parallel study of the DNSSEC signing, etc., should be conducted.

## 4. Technical and Process Improvements

### 4.1. Security Review

Several security-related improvements seem sensible.

p 32: "... a formal and documented Software Development Lifecycle (SDLC) inclusive of upfront security and resiliency requirements does not exist."

This is a long-standing gap and a major deficiency.

**Recommendation:** Get it done!

p 33: "We find that documentation of historical rationale, practice, and 'case law' is lacking..." In addition to the recommendations that are already included, do an annual review of all the events.

**Recommendation:** Augment the documentation as needed, update the training, and go through a formal consideration as to whether changes are needed in procedures, training, technology, etc.

p 34, 3rd para: "monitoring specifically for security events appears uneven...": What does this mean? (Included in section 5.2, Copy Editing, as well)

p 35, next to last para: What's the actual experience with respect to lack of availability? Delay is usually not a big problem.

p 47: Process Flows, Background

**Recommendation:** Annotate the process flows with quantitative data: volume, time, errors. Report annually.

p 48: Process Flows, Findings

**Recommendation:** Each failure or override should be documented and justified. If the check is out of sync with the needs, revise the check.

[6] [Study] p 26.

p 48: What about the label tables?

### 4.2. Technical Checks

The material on technical checks raises some questions.

p 18, q 4: What are the stats on false negatives? Have there ever been any false positives?

p 19: "IANA process documentation does not include criteria for decision making as to the completeness of an application." Why is this not completely and easily available to the clients?

p 39, Serial Number Consistency Check: Coherence needs to be more carefully and completely defined and checked. This probably requires some serious technical discussion and work with the community to arrive at a consensus. An IETF standard should result.

p 40, Other Technical Checks and Coaching vs. Auditing: Why aren't the checks completely open? TLD operators should have access to them, be encouraged to use them, and be offered assistance to learn and use the tools. The assistance need not come only from ICANN. It can also come from peers.

### 4.3. Update of DS and NS Records

There is considerable attention to IANA's policy and strategy regarding requiring DNSKEY records in the TLD zone before making changes to the corresponding DS record in the root. This seems to be a considered, careful, and appropriate strategy.

As a separate matter, there is a question of providing an API for large operators to issue change requests. Such an API would presumably facilitate changes to all records.
The challenge of automating updates in the parent zone is also being addressed for registries in general. Several ccTLDs are currently scanning for CDS and CDNSKEY records for automated updates of DS records. More recently, CSYNC records have been introduced to automate the update of NS and other records.

**Recommendation:** RZERC should consider whether such mechanisms based on CDS, CDNSKEY and CSYNC can be used for updates to the root zone as well. This would simplify implementation and leverage synergies from other DNS hierarchy layers, including broad deployment experience and testing by registries.

### 4.4. Statistics

It would be quite helpful to have a fuller statistical picture of the operation of IANA. Some of the statistics are included in the report as ancillary commentary.

A key statistic is that each TLD submits an average of one to two changes per year. On p 30 it's noted there have been 4600+ changes in the past 12 months, a significant increase. If I understand the numbers correctly, that seems like a factor of about two. What impact has that had on the load on the staff? On the response time?

Q2 in the survey asks a TLD operator whether they make changes (a) rarely or never, (b) 1-2 times per year, or (c) more than twice annually. This is probably a prelude to Q3, which asks for details. Nonetheless, IANA quite obviously has complete statistics, so it would be helpful to compare these responses with IANA's records.

Similarly, Q5 in the survey asks whether the time to complete updates is (a) about right, (b) too long, or (c) too quick. It would be helpful for the actual processing times, as seen from IANA, to be included.

p 47 describes the sub-processes for the Root Zone Management Change Request Process

**Recommendation:** It would be useful to annotate the process flows with the volume, response time, and error rates. Update and review annually.

### 4.5. IANA Staffing

p 45 shows the staffing for IANA. IANA provides three services, root zone updates, address block allocation, and IETF RFC registries. What is the division of staff across these three functions? I'm under the impression the number of RFC registry transactions per year is comparable to the number of root zone updates, and there are very few address block allocations per year.

p 33, under Training/Judgment/Process Errors, 3rd para: What's the depth in the staff and how well would it scale?

## 5. Edits for Clarity

### 5.1. Acronyms and Vocabulary

The report would benefit from a list of acronyms and terms. The following is a partial list of acronyms that didn't seem to be defined.

COTS: p 34. (Other places too)
GRC p 32
IFO
RM: p 49
RZCR p 30

## 5.2. Copy Editing

p 11, bullet: s/where/were/

p 27, 1st para under Description of the Processes, last line: s/as/has/

p 31: "in the case of DNS changes..." Is what's being excluded changes in contact data? If so, it would be clearer to say so.

p 31: next to last para: "critical TLD": Which TLDs are not critical?

p 32, next to last para: the last half of this para has already been stated, so this is redundant.

PTI is hardly mentioned. Most of the references are to ICANN and IANA. As noted in 2.1, Description of the IANA Process, it would be helpful to have an introduction of the organizational structure and the lines of responsibility. With the rest of the report, references to the various parties should be consistent. The same applies to Verisign vs. RZM.

p 34, 3rd para: "monitoring specifically for security events appears uneven...": What does this mean? (Included in section 4.1, Security Review, as well)

p 34, para 5: "ICANN also provided examples of their periodic business continuity exercises and their continuity of operations plan, here too these artifacts and exercises did not involve scenarios where a potential system compromise was in play necessitating ICANN invoke incident response detection, and response capabilities." This paragraph needs work. It probably needs to be broken into two or three sentences, and it's not clear what it's trying to say.

## References


[RFP] https://www.icann.org/en/system/files/files/rfp-root-zone-update-process-study-28apr20-en.pdf

[Study] https://itp.cdn.icann.org/en/files/internet-assigned-numbers-authority-iana-functions/rzm-study-jas-icj-14-03-2022-14-03-2022-en.pdf

[Glue] https://archive.icann.org/en/tlds/report-root-zone-glue-handling-nov09-en.pdf

[Ukraine] https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf