Table of Contents

Annex-2010-09-24-002 New-gTLD-Applicant-Support

ANNEX - Draft Excerpt Final Report New gTLD Applicant Support (JAS WG) [2010.09.24-002]

The WG decided that the initial focus should be on finding a relatively limited and identifiable set of potential applicants that would be not controversial to support. Unless otherwise indicated, the WG reached consensus on the following recommendations.

1. Recommendations on cost reductions

The WG recommends that the following fee reductions be made available to all applicants who are determined as meeting the need criteria established for financial support:

- Waive the cost of Program Development (US$26,000);
- Payment of the fees incrementally (perhaps following the refund schedule in reverse);
- Eliminate contingency fee of US$60,000;
- Decrement the US$100,000 fee so as not to make new gTLD applicants who meet the need criteria pay fee based on the expenses of the previous round. Without a full analysis of what went into calculating this cost it is difficult to estimate what percentage of these fees should be eliminated for qualifying applicants.

Further, the WG recommends that all applicants who are determined as meeting the need criteria established for financial support receive the following consideration:

- Qualified applicants receive a partial refund from any auction proceeds, should any become available;
- Lower the Registry fixed fees due to ICANN. In lieu of the Registry-Level fixed fee of US$25,000 per calendar year, only charge the Registry-Level Transaction Fee per initial or renewal domain name registration.

2. Recommendations regarding Sponsorship/ Fundraising

The group discussed the possibility of financial assistance for applicants. This was seen as coming from two types of sources:

- *Distributed by an ICANN originated fund* - It was uncertain what sort of funding might be arranged through ICANN, especially for this first round, though the group recommends that a fundraising effort be established. For any funding provided through ICANN by a benefactor that does not wish to administer that funding itself, these funds would be allocated by a specially dedicated committee, only to those who meet the need conditions established for the program;
- *From external funding agencies* - External funding agencies would make grants according to their own requirements and goals. ICANN would only provide applicant information to external funding agencies that met need conditions established by the program.

TLD applicants would be free to approach external funding agencies on their own initiative without affecting their applications for financial or other assistance under this program.

- The WG recommends that ICANN begin a search for a development director with an initial goal of securing commitments for US$10,000,000 for an ICANN based development fund;
- There was some support in the WG for recommending that ICANN put in place the means for existing registrants to voluntarily contribute to the development program through registrar-to-registry contribution pass-through, and enable non-registrant small donors to contribute to the

development program, and concurrent with the execution of the development message to the donor communities, that the development message also be delivered to the registrant, and non-registrant user communities through earned and paid media;
- The WG recommend working with well know development funding agencies to set up funding programs for gTLD for less developed region applicants who meet the needs-based criteria.

3. Recommendations regarding non-cost considerations

The members of the working group recommended that a program be initiated to enable the following types of aid to be provided to all applicants, especially those meeting the need conditions:
- Logistical support in the application process;
- Technical support for applicants in operating or qualifying to operate a gTLD.

4. Which applicants would be entitled to special support

The primary criterion for eligibility is financial need. The definition of financial need and the method for determining the needs of an application has not been established by the WG at this time. Among the types of applicant that are to be included in support, once financial or other need has been established are:
- Community-based applications such as cultural, linguistic and ethnic;
- Non-governmental Organizations (NGOs), civil society and not-for-profit organizations;
- Applicants geographically located in emerging markets/developing countries;
- Applications in languages whose presence on the web is limited;
- Entrepreneurs wanting to serve a developing market that might not be sustainable under the current cost structure.

NOT recommended for support, even if they can demonstrate financial need, are the following types of application:
- Geographic names;
- Purely Government/para-state applicants (though applicants with some Government support might be eligible);
- Applicants whose business model does not demonstrate sustainability.

5. Defined Constraints on aid

- On financial aid, no more that 50% of the financial aid for the reduced fee can be provided by an ICANN organized development fund. This is not meant to limit the manner in which fund raising for the other 50% is done and can include grant and aid from non ICANN related sources;
- Support should have an agreed cut-off/sunset point, e.g. 5 years, after which no further support would be offered;
- Support requests and levels should be made public to encourage transparency.
- The receipt of some support from government(s) should not disqualify an applicant from receiving gTLD support. However, the process is not designed to subsidize government-led initiatives;
- In cases where supported gTLDs make revenue significantly above and beyond costs, recipients would agree to re-pay/rebate application subsidies into a revolving fund to support future applications.

6. Relationship to the Application Guide

These recommendations should not affect the content of the Application Guide. Rather it is a separate program that needs to be established in parallel with the completion of the Application Guide Book.

7. Support for bundling

Note: There is an ongoing discussion within the Working Group as to whether this is in scope with the charter of the group. As that discussion has not yet been finalized, the issue is included here for information purposes.

There has been consensus to apply the following program to applicants that meet the criteria in 4. There is support, but no consensus to apply this program to all applicants. Based on recommendations within the group and from the comments there was no consensus but two proposals for bundling to support minority language applicants. The two proposals for bundling are discussed below.

Option A

In the case of applicants who are applying for one IDN gTLD, [a second IDN gTLD, further IDN gTLDs] would receive a discount application fee (from the full price for those who don't qualify for the need based criteria or the reduced price from those who do qualify for need based reduction) on sliding discount scale based on the number of native users of the script.

Option B

For the purposes of application fee calculation, the two or more strings shall be considered as a single application.

The WG advises applicants that there is, at present, no mechanism to completely and transparently deliver single administrative costs over two or more namespaces through CNAME, DNAME, or other means, and that service delivery to multiple namespaces is likely to have higher administrative costs than service delivery to a single namespace.

The WG advises that the intent of the WG is not to replace or create an alternative to any policy generally available for "variant characters" within a single script.

Annex-2010.09.24-003 Root-Zone-Scaling

Executive Summary

In February 2009, the ICANN Board requested a study be undertaken to examine the impact of the inclusion of a number of new technologies and the potential addition of significant numbers of new top-level domains to the root of the DNS. While some of these technologies had, by that time, already seen some deployment, some concerns were raised in the community that the stability of the DNS might be at risk if changes and additions were pursued without caution. As a result of the ICANN Board request, two studies were performed, one focusing on the impact of the new technologies and TLD additions on one root server, the other taking a wider view and looking at all processes associated with the management of the root system.

The new technologies of interest included IPv6 (both in terms of IPv6 addresses being associated with top-level domains and root servers as well as supporting IPv6 queries sent to the root servers), Internationalized Domain Names (IDNs), and security enhancements for the DNS (DNSSEC). However, since (and even in some cases, prior to) the ICANN Board resolution, all of these technologies have been deployed or implemented at the root, thus some empirical evidence exists which can be used in understanding the impact of these technologies.

To date, the deployment of IPv6, DNSSEC, and IDNs to the root system has had no significant harmful impact. While the deployment of these new technologies may have caused some minor degradation of service due to the lack of robust IPv6 infrastructure and/or the larger response size (due to the addition of IPv6 records or the DNSSSEC-signing of the root) causing that response to be dropped resulting in timeouts and retransmissions, no impacts were significant enough to have raised any concern among relevant communities.

Looking forward, with the assumption that estimates relating to a cap of less than 1000 new gTLDs per year being added to the root zone are accurate and assuming other parameters relating to the management of the DNS root are not altered substantively, it seems probable that normal operational upgrade cycles and resource allocations will be sufficient to ensure that scaling of the root, both in terms of new technologies as well as new content, will have no significant impact on the stability of the root system.

However, with the understanding that the management of the root of the DNS involves multiple parties and in the interest of the highest levels of care with respect to the stability of the root of the DNS, monitoring of root management system should be improved, particularly in the areas most sensitive to changes in rate of growth or which require significant lead-time in which to change. In addition, clearer and more frequent communication between relevant root management partners and other stakeholders, including formal communications between ICANN staff and root server operators regarding projected numbers of approved applications, additional technologies that need to be deployed and in what

timeframes, etc. would likely improve the confidence that changes to the root system won't negatively affect the stability of that system.

Introduction

Between 2004 and 2010, the root of the DNS has been undergoing significant change, both in terms of content as well as its support infrastructure. From the addition of Internationalized Domain Names (IDNs) in the root to the deployment of IPv6 and DNSSEC, it is safe to say that more change has occurred in the last 5 or 6 years than has occurred since the DNS was first deployed. With the imminent acceptance of applications for new generic Top-Level Domains (gTLDs), further substantive changes in the root of the DNS can be expected.

In keeping with ICANN's mission "to ensure the stable and secure operation of the Internet's unique identifier systems"[1] ICANN's Board requested a study to be performed jointly by ICANN's Root Server System Advisory Committee (RSSAC) and ICANN's Security and Stability Advisory Committee (SSAC) with support by senior ICANN staff to investigate the impact of the proposed modifications to the DNS root system. However, both prior to and during the implementation of this study, many of the changes in the root system of interest to the Board were already implemented with no observable negative consequences.

This paper provides a summarization of the changes that have occurred to the DNS root and provides an analysis of those changes along with estimates as to the projected impact of future changes including the addition of new top-level domains.

Background

On 3 February 2009, the ICANN Board unanimously resolved in resolution 2009-02-03-04[2] that a joint RSSAC and SSAC study be conducted to analyze "*the impact to security and stability within the DNS root server system of [the IPv6, IDN TLDs, DNSSEC, and new gTLDs] proposed implementations."* The resolution stated that the joint study should:

- "*[A]ddress the implications of initial implementation of these changes occurring during a compressed time period."*
- "*[A]ddress the capacity and scaling of the root server system to address a stressing range of technical challenges and operational demands that might emerge as part of the implementation of proposed changes."*
- "*[D]evelop a terms of reference for the Study and appoint a steering committee to guide the effort by 28 February 2009."*
- "*[I]nvolve direct participation by senior ICANN technical staff involved with its planned implementations of these activities and to provide necessary support to implement aspects of this study under terms and with ultimate approval of the advisory committees."*

---

[1] From "Article 1, Section 1. Mission" of ICANN's By Laws, see http://www.icann.org/en/general/bylaws.htm

[2] See http://www.icann.org/en/minutes/prelim-report-03feb09.htm

- Ensure *"the process for establishing the study terms, design and implementation will address the technical and operational concerns regarding expanding the DNS root zone that have been expressed on this topic."*
- Provide to the ICANN Board *"study findings and recommendations by 15 May 2009."*

As a result of this resolution, two efforts were undertaken, a study focused on the impact of scaling the root on one root server (the "L" root server operated by ICANN) and a more general study that aimed to model the processes in the root management system and analyze the results of scaling the system. An ad hoc study team known as the "Root Server Scaling Team" (RSST) was established comprised of members of RSSAC, SSAC, and outside experts to perform this second study.

The "L" Root Study

The "L" Root Study performed by the Domain Name System Operations and Research Center (DNS-OARC) under contract to ICANN focused specifically on the impact of different combinations of adding IPv6, DNSSEC, and new TLDs to a laboratory simulation of the "L" Root Server. The final report of this study, entitled "Root Zone Augmentation and Impact Analysis" was published on 17 September 2009 and is available at http://www.icann.org/en/topics/ssr/root-zone-augementation-analysis-17sep09-en.pdf.

The RSST Study

The RSST Study, which used the "L" Root Study as part of its input, outsourced the development of a simulation of root management processes, and conducted interviews with root server operators, IANA staff, VeriSign, NTIA, and others, was far more general, aiming to look at not only the impact on the root servers, but also on the provisioning systems that lead up to the root zone being propagated to the root servers. The final report of this study, entitled "Scaling the Root" with a sub-title of "Report on the Impact on the DNS Root System of Increasing the Size and Volatility of the Root Zone" was published on 31 Aug 2009 and is available at http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf.

Root Scaling Events

Prior to and since the ICANN Board requested SSAC, RSSAC, and senior ICANN staff to undertake the study of the implications of scaling the root, many of the subjects of that study have already been implemented. The timeline associated with the introduction of new technologies to the root is provided in Table 1.

Date	Technology	Event
July 2004	IPv6	First IPv6 addresses added to the root zone for top-level domains (KR and JP).
November 2005	DNSSEC	First top-level domain (.SE) signed.
June 2007	DNSSEC	IANA DNSSEC-signed root test bed made available.
August 2007	IDNs	Test IDN top-level domains added to the root.
February 2008	IPv6, gTLDs	First IPv6 addresses added for root servers (A, F, J, K, L, and M). A limit of a maximum of less than 1000 new gTLDs per year is derived from estimates of gTLD processing times.
January 2010	DNSSEC	Deliberately Unvalidatable Root Zone (DURZ) published on first root server ("L").
May 2010	IDNs, DNSSEC	First production IDNs added to the root (for Egypt, Saudi Arabia, and United Arab Emirates). DURZ deployed on all 13 root servers.
June 2010	DNSSEC	First DS records are published in the root zone (for .UK and .BR).
July 2010	DNSSEC	Root is DNSSEC-signed and the root trust anchor is published.

Table 1. Root Scaling Events

Impacts

During the period from July 2004 when the first IPv6 addresses were added to the root zone for TLD name servers until the root was DNSSEC-signed and DS records were inserted into the root in July 2010, root DNS service has continued with no reported or publicly visible degradation of service related to these events. This section examines the impact of each of the various changes to the DNS root.

IPv6

The inclusion of IPv6 in the root of the DNS has two components: adding IPv6 "glue" records[3] in the root zone for the authoritative name servers of TLDs and adding IPv6 "glue" records to the root servers. Each of these impacts will be examined in turn.

[3] Glue records are IPv4 ("A") and IPv6 ("AAAA") resource records associated with name servers that are in the zone being looked up. See RFC 1034 (http://www.ietf.org/rfc/rfc1034.txt) for the definition of glue records.

Top-Level Domains

In July 2004, the .JP and .KR domains were the first TLDs to have IPv6 "glue" records added. As of 6 September 2010, there are 283 IPv6 "glue" records in the root zone covering 203 TLDs. One impact of the increased use of IPv6 "glue" records has been an increase in the number of resolutions using IPv6 transport. As of 6 September 2010, at least one root server (the "L" Root Server) is seeing approximately 1.3% of DNS queries over IPv6[4]. Due to the less robust IPv6 network infrastructure within the Internet today, IPv6 queries and/or responses may be lost more frequently than with IPv4, resulting in more timeouts and retransmissions that would have occurred without IPv6 support in the TLDs. However, this impact has minimal negative consequences and is expected to improve as IPv6 deployment moves forward.

Root Servers

When some of the root server operators added IPv6 addresses for their root name server records, the size of the "priming query" increased significantly. As discussed in report produced jointly by RSSAC and SSAC labeled SAC018 and entitled "Accommodating IP Version 6 Address Resource Records for the Root of the Domain Name System"[5], there were concerns due to the fact that the priming response was anticipated to grow to more than the "classic" DNS maximal non-truncated response of 512 bytes. If the resolver requesting the priming response did not provide a larger response buffer size via the EDNS0[6] extension, it was feared the root servers might indicate a truncated response causing the requesting resolver to retransmit the request over TCP. Since TCP-based DNS queries are significantly more resource-intensive than the normal UDP-based queries, there was some concern that the root servers could be overloaded resulting in degradation of service to all users that queried the root servers. In addition, there was some concern that the larger response from the root servers would be blocked or filtered by firewalls, NATs, and other "middlebox" devices that "knew" (incorrectly) that a DNS response could never be more than 512 bytes. In such cases, there was a risk that the requestors might never receive a response and thus be unable to obtain the addresses of the root servers.

After significant study and testing of this issue, IPv6 addresses were added to the root zone in February 2008. In practice, the DNS server implementations running on the root discarded non-essential ("Additional Section") information in preference to truncating responses to queries that did not specify a sufficiently large buffer via EDNS0 (or did not use EDNS0). This may have resulted in a slight uptick in the number of queries sent to the root servers as resolvers were required to issue additional queries for data that had previously been supplied in the Additional Section, however if so, the increase was not noticeable.

---

[4] Private communication with the operators of the "L" root server. Other root servers should see a similar percentage of queries.

[5] See http://www.icann.org/en/committees/security/sac018.pdf

[6] EDNS0 is defined in RFC 2671 (see http://www.ietf.org/rfc/rfc2671.txt).

For those requestors that supplied a larger buffer size via the EDNS0 extension, there may have been an increase in the number of fragmented packets which could have resulted in dropped responses either due to the loss of a fragment or because middleboxes were configured to discard fragments. In addition, some security policies have suggested (erroneously) that TCP-based DNS should be blocked. In such cases, a priming query without the EDNS0 option (or in which the offered buffer was less than the size of the response) could result in an answer that was blocked. However, in the more than two and a half years since the first IPv6 "glue" records for the root servers were installed into the root, there have been no significant (if any) reports of negative consequences.

Looking at the processing side of the root management system, ICANN root management processes and system as well as VeriSign processes and systems required some modification to deal with the IPv6 "AAAA" resource records and to verify IPv6 reachability in "technical checks" performed by both parties. The impacts to both ICANN and VeriSign were minimal however and these processes and systems continue to operate today without incident.

Internationalized Domain Names

From the perspective of the DNS, aside from a slightly longer average label length, Internationalized Domain Names are essentially indistinguishable from any other domain name. The addition of IDNs to the root was thus no different to the DNS than adding any other non-IDN TLD to the root. As such, no impact at the DNS level was observed.

There was, however, some impact in ICANN root management processes and systems. In order to usefully display IDN information, IANA staff needed to revise processes to request U-labels in addition to A-labels and had to modify IANA systems such as the Whois server to support to display both A-labels and U-labels. More generally, the support of IDNs in backend systems, particularly in the display of registrant data, continues to be a topic of ongoing discussion in ICANN (and other, e.g., security-related) forums. It can be anticipated that the proper display of IDN information will be a non-trivial impact across (at least) registrars in the future.

DNSSEC

The addition of DNSSEC to the root had significant impact, both in terms of the size of the root zone, size of responses to root queries, as well as the implications deploying DNSSEC has had to ICANN, VeriSign, and NTIA, the parties involved in root zone management. In terms of root zone size, as of 6 September 2010, the signed root zone (as transmitted over the wire in a full zone transfer) was 222,246 bytes. When all DNSSEC-related records, namely DNSKEY, NSEC, DS, and RRSIG resource records, were stripped from that zone, the resulting zone size was 122,657 bytes. However, based on data from the "L" Root Study, it was anticipated that the additional data load on any reasonably configured name server imposed by DNSSEC would be inconsequential and in practice, this was borne out: there were no reports of any difficulties experienced by any of the root server operators loading and serving the DNSSEC-signed zone during the deployment of the "Deliberately

Unvalidatable Root Zone (DURZ)", the staged deployment of DNSSEC in the root prior to publishing the root trust anchor.

Potentially more significantly, the size of the majority of responses from the root servers grew by a non-trivial amount, e.g., a query for the root name servers went from 492 bytes to 829 bytes when a DNSSEC-signed response was requested. As opposed to zone data size, a doubling of the size of a DNS response was of concern due to the 512-byte limit discussed previously in the context of IPv6. The DNSSEC specifications addressed this limit by requiring the use of EDNS0 to signal the resolver was equipped to handle responses that included DNSSEC-related resource records. However, as it turns out, most resolvers on the Internet, at least those querying the root servers, by default use EDNS0 and set a bit in DNS queries (the "DNSSEC OK" bit) to indicate the resolver understands responses that include DNSSEC-related resource records (regardless of whether or not the resolver will make use of those resource records). As a result, between 50% and 80% of the queries hitting the root server prior to the root being signed had the "DNSSEC OK" bit set and thus, when the signed root was served from all the root servers, those servers immediately started returning an aggregate of at least 50,000 DNSSEC-related resource records per second[7].

Prior to the root being signed, significant concerns existed regarding the impact of the larger DNSSEC-signed responses being returned to clients who may not be expecting them. In particular, there were concerns that middleboxes would, like in the case of IPv6 mentioned earlier, discard responses larger than 512 bytes. As a result, ICANN, VeriSign, and NTIA agreed upon a phased deployment of the signed root zone (the "DURZ") that also included substantial instrumentation of root servers to observe any change in query patterns. However, after deploying the signed root zone to all 13 root servers over the course of 6 months, no reports of negative consequences were received by any of the parties involved in signing the root.

In terms of process changes, deployment of DNSSEC at the root resulting in the creation of elaborate new processes along with new physical facilities that are necessary to securely manage the root key-signing key by ICANN and the root zone-signing key by VeriSign. New processes were also established to allow TLD administrators to securely provide "delegation signer" (DS) information to ICANN (and to allow ICANN to submit DS information to VeriSign for inclusion in the root zone) to enable the creation of a "chain of trust" from the root to signed child zones. To date, these new processes have operated without incident.

[7] Assuming a back-of-the-envelop estimate of an average of 8000 queries per second per root server cluster over 13 root server clusters and with the "DNSSEC OK" bit set in half the queries.

Summary

Summarizing the impacts to date of the addition of IPv6 to the root system, IDN top-level domains, and the deployment of DNSSEC, no significant harmful effects have either been observed by or reported to ICANN.

However, with that said, one point that has been raised in the context of discussions regarding root scaling is the need for improved communications between stakeholders involved in the management of the root system. In some cases, the introduction of new technologies could likely have been improved with more formal communication of requirements from all parties that may have been impacted, discussion of those requirements and impacts, documented plans with timelines, etc. The communications, documentation, and discussions surrounding the deployment of the signed root have been suggested as an example of movement in the right direction in this regard.

Projections

The root system continues to undergo changes, albeit now more in terms of continued deployments of existing technologies than in structural changes such as the introduction of new technologies. This section examines some projections of likely changes, making the assumption that parameters such as zone refresh times, DNS record Time-To-Live (TTL) values, rates of root zone changes, and the length and complexity of administrative processes do not vary wildly or unexpectedly from historical values.

IPv6

It is highly likely that in the future, additional top-level domains will add IPv6 address records for their name servers. As of 6 September 2010, the root zone contains 283 IPv6 "glue" records corresponding to 203 out of 294 top-level domains having at least one IPv6 address record for their name servers. As IPv6 becomes more fully deployed, it is safe to assume more TLDs will be adding IPv6 support, eventually to cover all TLDs, and that the average number of IPv6-supporting name servers for those TLDs will go up. Until the Internet's IPv6 infrastructure improves to be on par with the IPv4 infrastructure, end users may experience some negative consequences in the form of delays resulting from queries sent to IPv6 name servers timing out.

In the case of the root, SAC018 documents that the size of the priming query response when all root servers have deployed IPv6 should be 811 bytes. While the root server operators that have not yet deployed IPv6 have not provided dates when they plan on enabling IPv6 on their root servers, they have all indicated they do intend to do so[8]. However, since larger than 512 byte responses have already been encountered, the additional 100+ bytes in a priming query response is unlikely to have noticeable impact.

[8] Private communications with the co-chair of RSSAC and with the operator of the "L" root server.

DNSSEC

As of 15 July 2010, the root zone has been signed and is being distributed to all instances of all 13 root servers. As such, further impact to the root zone from DNSSEC is likely to be limited to the addition, modification, and deletion of Delegation Signer (DS) resource records, the potential for changes in key algorithms, key lengths, or number of keys, and key rollover events.

Since DS resource records can vary in size based on the hashing algorithm used, the exact increase in size the addition of DS records will have in the future is difficult to accurately predict. However, given the structure of DS resource records, it can be argued that a pessimistic estimate of DS record size would be 64 bytes. As of 6 September 2010, there are 49 DS records for 29 TLDs (including the 11 test IDN TLDs still in the root). Assuming, as the "L" Root study does, that full deployment of DS records by TLDs will result in a total of 1440 DS RRs for 1000 zones, the total number of bytes DS records will add would be less than 100 Kbytes. The actual number will likely be significantly less as it is tied to the number of TLDs and, as discussed in the subsequent section, this number is expected to be significantly less than the 1000 new TLDs assumed in the "L" Root study.

With regards to changes in key algorithms, key lengths, and number of keys, it is possible that the most significant change will be to move to Elliptic Curve Cryptography, which will result in significantly smaller keys at the same cryptographic strength.

Finally, while it is more of an operational issue than a root scaling issue, key rollover events occur with some regularity with all DNSSEC-signed zones. In the normal course of events, key rollovers of key-signing keys will require updated DS records to be provided to the parent zone administrator. In the case of the root zone, rolling the root key-signing key will require updating the root trust anchor in all resolvers configured for validation. It is hoped that RFC 5011-based mechanisms will enable much of the root key-signing key rollover to be automated, but it can be anticipated that some disruption will occur when the root key-signing key is changed and thus, rolling the root key-signing key should be done with some care.

Top-Level Domains

In the analysis done in the draft document "Delegation Rate Scenarios for new gTLDs"[9], ICANN staff estimates that the expected rate of new TLDs entering the root will be on the order of 200 to 300, even with higher than anticipated application rates. The same paper infers that regardless of the number of applications, there will be a process-imposed limit in the addition of new TLDs of less than a maximum of 1000 new gTLDs per year[10]. For the purposes of this analysis, a fixed number of 1000 per year additional new TLDs will be assumed.

---

[9] See http://www.icann.org/en/topics/new-gtlds/anticipated-delegation-rate-model-25feb10-en.pdf

[10] 924 new TLDs per year to be specific.

Based on work done in the "L" Root study, the anticipated size of the DNSSEC-signed root zone with IPv6 and full DS deployment and with 1000 new top-level domains is 624,791 bytes. Based on input received from root server operators, it is unlikely this amount of zone data will stress any of the root servers. In addition, this root zone must be distributed to each instance of all 13 root servers. For the sake of this analysis, making the assumption that the effective minimum bandwidth (taking into consideration line noise, interrupted communications, etc.) to the worst connected instance of all root servers is 300 bits per second, it would take approximately 4 and a half hours to transfer the entire zone, well within the current 12-hour root zone regeneration period[11].

Looking forward 10 years, and still assuming a maximum of 1000 new TLDs per year, the "L" Root study projects the root zone will have grown to 7,471,784 bytes. Again, based on input from root server operators, it is unlikely this amount of zone data will stress any of the root servers. With regards to bandwidth, the minimum bandwidth necessary to transfer the zone of this size in the 12-hour window would be approximately 1400 bits per second.

Another potential future impact of the addition of new TLDs is related to root query "splay". That is, the dispersion of queries across an increased number of TLDs may have some impact on the operation of individual caching servers. While it is not certain that an increased number of TLDs will result in an increased number of queries or that query patterns will change drastically, taken to an extreme, if a resolver sends a query to each TLD in the root, the cache of that resolver will end up holding the NS records for each TLD (along with IPv4 and IPv6 "glue" records and DNSSEC-related records if they exist) for the duration of the Time-To-Live (TTL) of those records. Compared to the limited number of TLDs today, this would increase the amount of memory consumed by the caching name server and, depending on caching name server's memory management techniques, could increase the likelihood that the caching name server could run out of memory. However, caching name servers already must cope with these sorts of memory management challenges since there are already sufficient domain names that can be queried (at all levels) to overflow pretty much any memory configuration if queries are asked quickly enough (that is, within the TTLs of the records such that more new records are added than records are expired). As such, the impact associated with a higher degree of "splay" within the root zone is not expected to result in significant impact on caching servers.

As discussed in the RSST report, the addition of new top-level domains will likely have impacts related to processes and back end systems in use by ICANN (in performance of the IANA function), VeriSign, and NTIA. For example, the quantities of data maintained in the database used to maintain contact information for TLD administrators is likely to increase significantly and the processes used to vet

[11] 300 bits per second is, of course, an unrealistically low number, however a more realistic number would allow for the zone to be transferred more quickly thus the use of 300 bits per second could be considered a worst case.

requests at each of the organizations involved in root management will likely need to change to cope with the increased load associated with day-to-day root zone modifications. However, all of the organizations involved in root management have indicated that they will adjust their resources to meet demand. The primary consideration thus becomes detecting the increased loads prior to them becoming an issue and to facilitate the adjustment of resources. As such, monitoring of root management systems at points in those system where bottlenecks may arise as well as defining thresholds that signal areas of concern is an area in which additional efforts are required.

Summary

Predicting the future is known to be somewhat challenging, however in the case of projecting the impact of scaling the root, it seems likely that if we assume historical patterns don't change in unanticipated ways, anticipated growth is well within the capacity of the system to adjust to that growth.

In the case of IPv6, nearly 70% of top-level domains have already deployed IPv6 as has 8 of the 13 root servers. It is unlikely that moving to 100% of both of these will have any negative consequences (modulo possible delays to end users resulting from timeouts due to the IPv6 infrastructure not yet being on par with the IPv4 infrastructure).

With DNSSEC, while there will be additions of new DS records as more TLDs sign their zones, it is unlikely this will cause any noticeable change in the root other than the root zone getting larger at a rate that will be (at most) tied to the number of new TLDs.

Finally, the addition of new TLDs has the potential for the greatest impact, however given the projected limit of less than 1000 new TLDs per year; it is unlikely the impact of this growth will cause any disruption as long as systems and processes are adjusted as part of normal operational upgrades.

Conclusion

As the DNS continues to grow and evolve to meet new requirements, ensuring that those changes do not negatively impact the stability of the DNS is of critical importance. As a result of ICANN Board resolution 2009-02-03-04, two studies were undertaken to analyze the impact of the addition of IPv6, DNSSEC, IDNs, and new gTLDs to the root of the DNS. In the "L" Root study, it was shown that at least one root server could easily handle both the deployment of the new technologies as well as several orders of magnitude more new TLDs than are anticipated to even be possible to be processed by ICANN for the foreseeable future. The RSST study suggested that absolute numbers weren't particularly relevant, rather it was the rate of change and how various root management processes and back end systems are modified to deal with the changes that is important.

However, in the time between when resolution 2009-02-03-04 was issued and today, deployment of new technologies has continued, thus empirical data can be used to validate the observations of both studies. Deployment of IPv6 in the root,

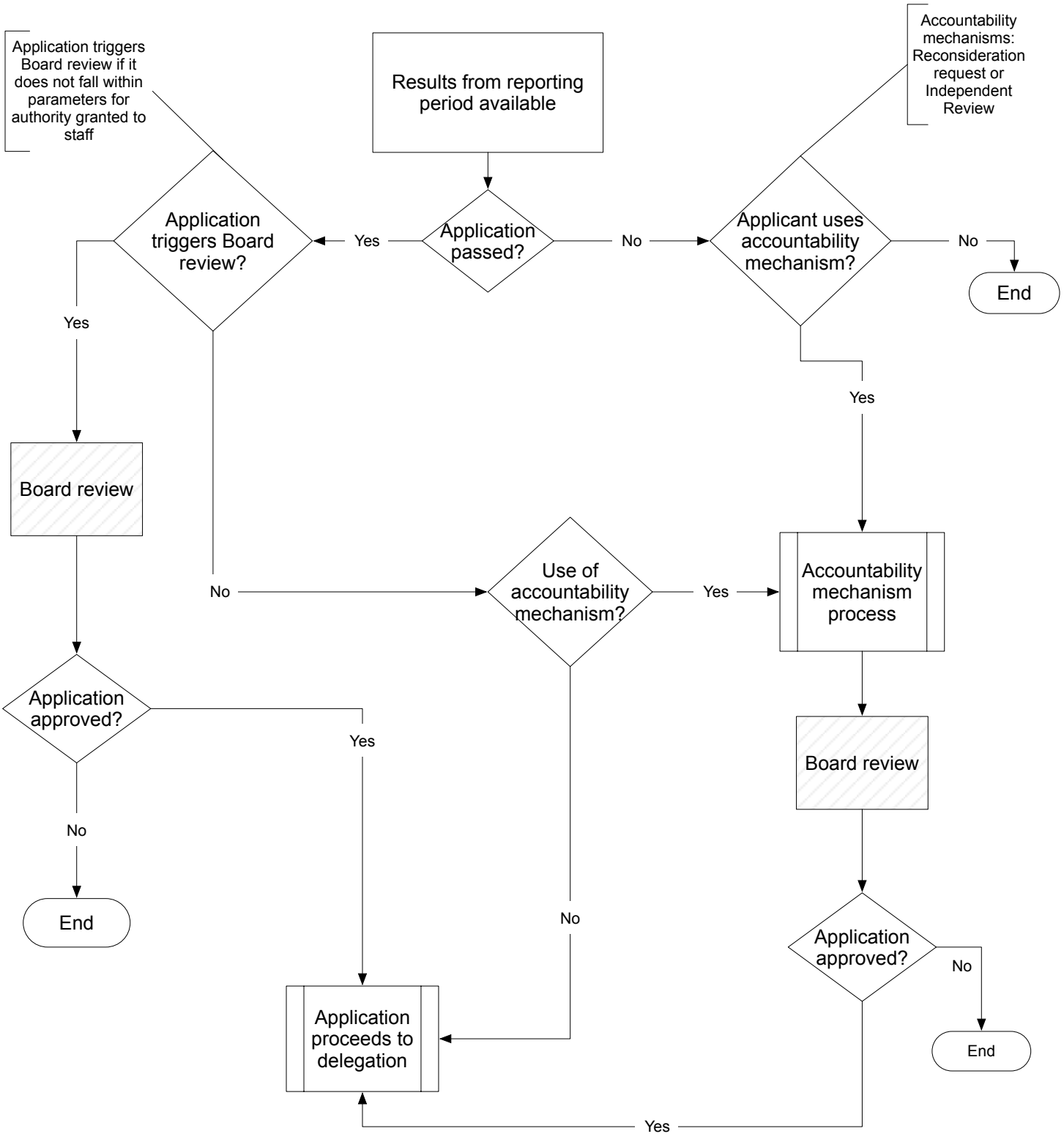
which began in 2004, has caused no significant harmful effects. Insertion of IDNs into the root in 2007 similarly was a non-event from the perspective of stability of the DNS, and deployment of DNSSEC in the root starting in January 2010 resulted in no observable or reported negative consequences.

Looking forward, further additions of IPv6, DNSSEC, and IDNs are unlikely to have any negative impact on the stability of the DNS, albeit the roll of the root key-signing key will need to be managed carefully to ensure validating resolvers have the new root trust anchor configured before the old trust anchor becomes invalid. The only remaining wildcard is related to the number of new TLDs inserted into the root.

One clear observation from the studies performed in response to ICANN Board Resolution 2009-02-03-04 and discussions related to those studies was that both monitoring of root management systems as well as communications between the various stakeholders involved in root management should be improved. While modifications to the root have, to date, not resulted in noticeable negative impact, it can be argued that without additional monitoring and improved communications, scaling of the root could pass a critical threshold without notice, resulting in scalability problems that could affect the stability of the DNS as a whole. With the assumptions that less than 1000 new TLDs will be added per year and that monitoring and communications among relevant stakeholders is improved, it seems clear that the root system should remain stable as it changes to meet new demands.

Annex-2010-09-24-007 Board-Role

Annex - Approval Process (Draft) [2010.09.24-007]



As shown here, there are two paths whereby an application would be reviewed by the Board:

1) Where the application does not fall within the parameters where staff is granted authority to proceed
2) As a result of an accountability mechanism used with regard to the application

Annex-2010-09-24-008 Mitigating-Malicious-Conduct

Annex: Mitigating Malicious Conduct [2010.09.24-008]

A. Recommendations for Mitigating Malicious Conduct

The nine recommendations proposed for implementation as a result of the consultations on mitigating malicious conduct are:

1. ***Vetted registry operators (i.e., background checks)*** – This recommendation requires that new gTLD applicants be appropriately reviewed, to determine if the potential registry operator has a criminal or malicious history.
2. ***Demonstrated plan for DNSSEC deployment –*** This recommendation requires that DNSSEC be deployed in new gTLDs, in order to reduce the risk of spoofed DNS records.
3. ***Prohibition of wildcarding*** – This recommendation requires appropriate controls around DNS wildcarding to reduce the risk of DNS redirection to a malicious site.
4. ***Removal of orphan glue records*** – This recommendation requires that new gTLD operators remove name server records when a domain name is removed from the gTLD, to reduce the risk of use of these remnant records by a malicious actor.
5. ***Requirement for thick WHOIS records*** – This recommendation requires that new gTLDs maintain and display "thick" Whois data, to improve the accuracy and completeness of the Whois database. The availability of thick Whois records provides a key mechanism to combat malicious use of the new gTLDs, by providing a more complete chain of contacts within the TLD. This in turn should allow for more rapid data search and resolution to malicious conduct activities, as they are identified.
6. ***Centralization of zone-file access*** – This recommendation requires that access credentials to obtain registry zone file data be made available through a centralized source, allowing for more accurate and rapid identification of key points of contact within each TLD. This reduces the time necessary to take corrective action within TLDs experiencing malicious activity.
7. ***Documented registry level abuse contacts and procedures –*** This recommendation requires that new gTLDs establish a single point of contact responsible for the handling of abuse complaints and provide a description of their policies for combating abuse. These requirements are considered fundamental steps in enabling successful efforts to combat malicious conduct within the new gTLDs.
8. ***Participation in an expedited registry security request process*** – This recommendation provides that new gTLD operators be enabled to take quick, effective actions in light of systemic threats to the DNS by establishing a specific process to review and approved expedited security requests.
9. ***Draft framework for high security zone verification*** – This recommendation suggests the creation of a voluntary program designed to designate TLDs wishing to establish and prove an enhanced level of security and trust. The overall goal of the program is to provide a mechanism for TLDs that desire to distinguish themselves as secure and trusted, for TLD business models that would benefit from this distinction.

B. Draft Applicant Guidebook provisions concerning background checks

This includes two relevant sections of the Applicant Guidebook revised to provide additional information on background checks.

- Section 1.2.1 is part of Module 1 (Introduction) and describes eligibility factors for all applicants. This section has been revised to include an expanded description of the rationale for the background screening requirements, and to include an enumerated list of disqualifying factors (items i-xiii).

- Section 2.1 is included in Module 2 (Evaluation Procedures) and describes the process that ICANN will use to perform the background screening. This process covers two areas:

    - General business diligence and criminal history. Any applicant entities listed and in good standing on any of the world's 25 largest stock exchanges will be deemed to have passed the general business diligence and criminal history screening. The stringent requirements for public listing on these exchanges make additional screening by ICANN of limited value. For all other applications, ICANN will submit identifying information for the entity, officers, directors, and major shareholders to an international background screening vendor. This vendor will only return "hits" from public information that match the criteria listed in section 1.2.1.

    - Domain-name-specific behavior. Recognizing that operation of a domain namespace presents unique opportunities for unacceptable behavior, ICANN will screen applicants against UDRP cases for domain-namespace-specific data that may indicate a history or pattern of such behavior. Additional criteria for considering the results of UDRP case history are being developed and will be included in the guidebook.

1.2.1 Eligibility

Established corporations, organizations, or institutions in good standing may apply for a new gTLD. Applications from or on behalf of yet to be formed legal entities, or applications presupposing the future formation of a legal entity (for example, a pending Joint Venture) will not be considered. Applications from individuals or sole proprietorships will not be considered.

ICANN has designed multiple stakeholder protection mechanisms in the New gTLD Program. During the application process, general business due diligence is performed to determine that the applicant is organizationally, legally, technically, and financially capable of performing the required duties. The extensive technical and financial reviews detailed in the guidebook are proactive mechanisms; additionally, background screening is a proactive mechanism to find indications that an applicant may be a bad actor. After delegation, numerous features of the gTLD Registry Agreement together with technical and financial escrow mechanisms provide substantial registrant protection for a range of potential issues that may arise during operations. When viewed as a whole, the protection mechanisms ICANN has put in place provide a proactive and reactive "defense in depth" strategy to protect the entire stakeholder community.

The application form requires applicants to provide information on the legal establishment of the applying entity, as well as the identification of directors, officers, partners, and major shareholders of that entity.

Background screening at both the entity level and the individual level will be conducted for all applications to confirm eligibility. This inquiry is conducted on the basis of the information provided in questions 1-11 of the application form. ICANN will perform background screening in two areas: (1) General business diligence and criminal history; and (2) History of improper domain-name-specific behavior.

Background screening is in place to help protect the public interest in the allocation of critical Internet resources, and ICANN reserves the right to deny an otherwise qualified application, or to contact the applicant with additional questions, based on the information obtained during the background screening process.

While Applicants with confirmed offences of the types listed in (i) – (xiii) below will not be automatically disqualified from the program, ICANN is strongly predisposed against accepting such applications and would accept such an application only in rare and extenuating circumstances. Potential Applicants should bear this in mind prior to submitting an Application.

Circumstances where ICANN may deny an otherwise qualified application include, but are not limited to instances where the applicant, or any partner, officer, director, or manager, or any person or entity owning (or beneficially owning) fifteen percent or more of the applicant:

(i) Within the past ten years, has been convicted of a felony, or of a misdemeanor related to financial or corporate governance activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that ICANN deemed as the substantive equivalent of any of these;

(ii) Within the past ten years has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of the funds of others;

(iii) Within the past ten years has been convicted of any willful tax-related fraud or willful evasion of tax liabilities;

(iv) Within the past ten years has been convicted of perjury, forswearing, failing to cooperate with a law enforcement investigation, or making false statements to a law enforcement agency or representative;

(v) Has ever been convicted of any crime involving the use of a weapon, force, or the threat of force;

(vi) Has ever been convicted of any violent or sexual offense victimizing children, the elderly, or individuals with disabilities;

(vii) Has been convicted of aiding, abetting, facilitating, enabling, conspiring to commit, or failing to report any of the listed crimes within the respective timeframes specified above;

(viii) Has entered a guilty plea as a part of a plea agreement or has a court case in any jurisdiction with a disposition of Adjudicated Guilty or Adjudication Withheld (or regional equivalents) for any of the listed crimes within the respective timeframes specified above;

(ix) Is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in (i) - (viii);

(x) Is the subject of a disqualification imposed by ICANN and in effect at the time the application is considered;

(xi) Fails to provide ICANN with the identifying information necessary to confirm identity at the time of application and/or to resolve questions of identity during the background screening process;

(xii) Is the subject of a pattern of decisions indicating liability for, or repeated practice of bad faith in regard to domain name registrations, including:

- (a) acquiring domain names primarily for the purpose of selling, renting, or otherwise transferring the domain name registrations to the owner of a trademark or service mark or to a competitor, for valuable consideration in excess of documented out-of-pocket costs directly related to the domain name; or
- (b) registering domain names in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name; or
- (c) registering domain names primarily for the purpose of disrupting the business of a competitor; or
- (d) using domain names with intent to attract, for commercial gain, Internet users to a web site or other on-line location, by creating a likelihood of confusion with a trademark or service mark as to the source, sponsorship, affiliation, or endorsement of the web site or location or of a product.

(xiii) Fails to provide a good faith effort to disclose all relevant information relating to items (i) – (xii).

All applicants are required to provide complete and detailed explanations regarding any of the above events as part of the application. Crimes of a personal nature that do not meet any of the criteria listed in (i) – (viii) will not be considered for the purpose of criminal background screening and do not need to be disclosed. Arrests, adjudications dropped or resulting in acquittal or dismissal, accusations, hearsay, and information having a primary source other than lawful courts, governments, regulatory agencies, or law enforcement agencies will not be considered for the purpose of background screening.

2.1 Background Screening

Background screening will be conducted in two areas:

(1) General business diligence and criminal history; and

(2) History of improper domain-name-specific behavior.

The criteria against which background screening results will be evaluated are described in Section 1.2.1. The following sections describe the process ICANN will use to perform background screening.

2.1.1 General business diligence and criminal history

Applying entities that are publically traded corporations listed and in good standing on any of the world's largest 25 stock exchanges will be deemed to have passed the general business diligence and criminal history screening.

Before an entity is listed on an exchange, it must undergo significant due diligence including an investigation by the exchange, regulators, and investment banks. As a publically listed corporation, entities are subject to ongoing scrutiny from shareholders, analysts, regulators, and exchanges. All exchanges require monitoring and disclosure of material information about directors, officers, and other key personnel including criminal behavior. In totality, the requirements, demands, and diligence a publically listed corporation is subject to far exceed the screening ICANN is capable of performing, making additional screening of limited value. Finally, as a practical matter, conducting background investigations on (possibly numerous) directors and officers of large multinational corporations is often unfeasible.

ICANN will accept evidence of listing and good standing on any of the world's largest 25 stock exchanges in lieu of general business diligence and criminal history screening. The exchanges are:

NYSE Euronext (US)
Tokyo SE Group
NASDAQ OMX
NYSE Euronext (Europe)
London SE
Shanghai SE
Hong Kong Exchanges
TSX Group (Toronto)
BME Spanish Exchanges
BM&FBOVESPA
Bombay SE
Deutsche Börse
Australian SE
National Stock Exchange India

SIX Swiss Exchange
Shenzhen SE
Korea Exchange
NASDAQ OMX Nordic Exchange
Johannesburg SE
MICEX (Russia)
Taiwan SE Corp.
Borsa Italiana
Singapore Exchange
Mexican Exchange
Saudi Stock Market – Tadawul

An application providing acceptable evidence of a listing in good standing on one of the above listed exchanges will proceed to screening for history of improper domain-name-specific behavior.

For applicants not listed on one of these exchanges, ICANN will submit identifying information for the entity, officers, directors, and major shareholders to an international background screening vendor. This vendor will be provided with the criteria listed in Section 1.2.1 and instructed to only return "hits" from public information that match these criteria.

Note that the applicant is expected to disclose potential "hits" in the application and provide any clarification of anticipated "hits" at the time of application submission. If any "hits" are returned, the application will be matched with the disclosures provided by the applicant and those issues will be followed up to resolve issues of potential false positives. If no "hits" are returned, the application will proceed to screening for history of improper domain-name-specific behavior.

2.1.2 History of improper domain-name-specific behavior

Recognizing that operation of a domain namespace presents unique opportunities for unacceptable behavior, ICANN will screen applicants against UDRP cases for data that may indicate a history or pattern of such behavior pursuant to the criteria listed in Section 1.2.1. Recognizing that the UDRP dataset requires interpretation, any "hits" will cause the application to be subject to further analysis. An absence of "hits" will allow the application to progress to the next application processing step.

Annex-2010-09-24-010 New-gTLD-Budget

Annex – New gTLD Program Budget [2010.09.24-010]

Adjustments to the New gTLD Budget posted 1 June 2010 are as follows:

Deployment Budget:

Activity	Estimated Cost	Adjustment	Revised Cost
A) Completion of application processing activities including process integration & software license fees	$0.7 million	$0.6 million	$1.3 million
B) Panelists on boarding including training development and delivery	$1.5 million	$0.1 million	$1.6 million
C) Global Communication Campaign	$0.3 million	$0.2 million	$0.5 million
D) Administration	$0.1 million	-	$0.1 million
Total	**$2.6 million**	**$0.9 million**	**$3.5 million***

Adjustment A) $0.6 million represents contingency planning for the overall gTLD program, additional security assessments for TAS, and securing additional resources such as the Independent Objector, URS, Trademark Clearinghouse, and other international resources

Adjustment B) $0.1 million represents the cost increase for on-boarding of Independent Objector, URS, and Trademark Clearinghouse resources and integration assistance with certain Dispute Resolution Service Providers

Adjustment C) $0.2 million represents the cost increase associated with providing education and application assistance to certain applicants as defined by the Applicant Support Working Group

* A 10% contingency budgetary line item, consistent with budgetary practices at ICANN, will be discussed with the BFC. If approved, this will increase the deployment budget to $3.85 million.

Application Processing Budget:

Activity	Total (,000)	Adjustment (,000)	Revised Total (,000)
Application Fees (@$185k)	$92,500.0	-	$92,500.0
Less: Risk Costs (Contingency Reserve @ $60k)	$(30,000.0)	-	$(30,000.0)
Development Costs (Recovery @ $25k)	$(12,500.0)	-	$(12,500.0)
Refunds	$(8,260.3)	-	$(8,260.3)
Net Revenue	$41,739.8	-	$41,739.7
Operating Expenses			
Variable			
Travel & Meetings	$(83.2)	-	$(83.2)
Professional Services			
1) Program Administration	$(2,047.9)	$(100.0)	$(2,147.9)
2) Initial Evaluation Panels	$(18,306.6)	$(105.0)	$(18,411.6)
3) Quality Control	$(2,462.5)	-	$(2,462.5)
4) Extended Evaluation Panels	$(769.3)	-	$(769.3)
5) Independent Objector	$(4,687.5)	-	$(4,687.5)
6) String Contention	$(431.1)	-	$(431.1)
7) Pre-Delegation	$(6,300.4)	-	$(6,300.4)
Fixed			
Personnel - gTLD Team	$(2,858.9)	-	$(2,858.9)
Personnel - ICANN Staff	$(3,296.0)	-	$(3,296.0)
Administration	$(311.9)	-	$(311.9)
Total Operating Expenses	$(41,555.2)	$(205)	$(41,760.3)
Total	**$184.6**	**$(205.0)**	**$(20.6)**

Adjustment to 1) Program Administration - $100k represents additional customer service costs to assist certain applicants, as defined by the Applicant Support Working Group, with the completion of the application

Adjustment 2) Initial Evaluation Panels - $105k represents the increase in costs to conduct background checks

Annex-2010-09-24-012 Vertical-Integration

ANNEX: Vertical Integration [2010.09.24-012]

Exhibit A: Evaluation of Vertical Integration Options (Salop and Wright)

Exhibit B: Redacted

Exhibit A:

Evaluation of Vertical Integration Options

DRAFT: 09/12/2010

Evaluation of Vertical Integration Options Proposed in the Initial Report on Vertical Integration Between Registrars and Registries

Steven C. Salop

Joshua D. Wright[1]

ICANN has requested that we review and analyze the six policy proposals discussed in the Initial Report prepared by the Vertical Integration PDP Working Report and ICANN Staff, which was delivered to the GNSO Council. ICANN also has requested that we review our own proposal ("SW") and compare it to these alternatives.[2] As part of this comparison, we will explain why we prefer our original proposal, as well as why we would recommend certain changes to it based on what we have learned from the other proposals.

I. Basic Economic Framework

[1] The authors are (respectively) Professor of Economics and Law, Georgetown University Law Center; Associate Professor, George Mason University School of Law and Department of Economics. Both authors are Senior Consultants, Charles River Associates.

[2] The Initial Report draft is dated July 23, 2010. The policy proposals discussed, according to the Initial Report, are those that "have garnered minimal levels of support and are actively under consideration." While the SW proposal was not explicitly included, at least one of the proposals considered by the Working Group is somewhat based on it.

The U.S. Supreme Court has characterized antitrust as a "consumer welfare prescription."[3] As economists steeped in antitrust analysis, we focus on the competitive effects the various proposals on registrants. This is an important issue because the various proposals differ with respect to their impact on the welfare of registrants, registries and registrars. In our view, ICANN policy towards the registries and registrars should be focused exclusively upon consumer welfare. The welfare of the registries and registrars matters to the extent that it is harmonized with the welfare of registrants.[4] The rules should protect competition, not competitors.

Economic analysis teaches that vertical integration and vertical contracts between registries and registrars can create both competitive benefits and competitive harms. Assessing the likely competitive effects of any particular contractual arrangement between a registry and registrar is a difficult and complex task. It is complicated by the fact that both the benefits and the harms sometimes may occur without cross-ownership. A registry or registrar can exercise its market power even when there is vertical separation.[5]

A vertically integrated registry owner (i.e., a registry that owns a registrar, or vice versa) may have the beneficial incentive to charge a lower registration fee. Vertical integration also might vitalize a struggling registry through the creation of a superior registry product. Vertical promotional agreements between registrars and registries are

[3] Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979). In this matter, the registrants are the "consumers."

[4] Our focus on consumer welfare analysis, for example, would count as a competitive benefit of vertical integration the potential for reduced costs and lower prices, despite the fact that lower prices offered by an integrated firm might result in competition that harms rival, unaffiliated registries.

[5] Vertical contracts can have effects like vertical integration. For example, a registrar with market power could charge registries a high price for access to its shelf space and an unintegrated registry with market power could charge registrars a high registration fee.

common today. They appear to be pro-competitive, and are capable of driving a significant increase in registrations. Where these efficiencies exist, they could cause harm to competing registries and registrars, but they would be beneficial for consumers.

However, vertical integration also can lead to the exercise and enhancement of market power. Under certain conditions, a dominant registrar with an ownership interest in a registry could refuse to promote competing registries and thereby allow its affiliated registry to gain market power or enhance the market power it has. Similarly, a dominant registry could withhold its domain (or other information) from competing registrars and thereby allow its affiliated registrar to gain or enhance its market power. Thus, a key factor in predicting whether vertical integration is capable of generating competitive harms is whether or not a registry or registrar has market power.[6]

Vertical integration also has the potential to facilitate the misuse of sensitive competitive information by vertically integrated registrar/registries. This could involve, for example, gaining information about rivals' plans to introduce innovative new services (or lower prices), which would permit a faster competitive response. The more rapid competitive response could benefit consumers if the innovations (or lower prices) are actually implemented; however, an unintegrated rival might anticipate that a competitor will be able to respond very quickly, thus reducing the profits from innovation and potentially dampening the incentive to innovate (or cut price).

Misuse of competitively-sensitive information also could cause other effects that have more mixed competitive effects. For example, if a vertically integrated registrar is

[6] Market power on the sell-side or the buy-side is a *necessary* but not *sufficient* condition for the possibility of such harms from vertical integration. *See generally* Michael H. Riordan & Steven C. Salop, Evaluating Vertical Mergers: A Post-Chicago Approach, 63 Antitrust Law Journal 513 (1995).

able to gain better access to expired domain names than other registrars, it could "taste" the domains within their affiliated registrar, and thereby gain an advantage in the market. This advantage would come at the expense of other, unaffiliated registrars. If this advantage causes other registrars to exit from the market or reduces their incentive to invest, competition and registrants could be harmed; if the advantage is not that severe, it could lead to increased investment in registries because the integrated registry/registrar would earn higher profits.[7] However, such activities can occur with or without integration. Further, to the extent there is a concern that it is harder to detect this conduct for a vertically integrated firm, that concern might be addressed a number of ways, including internal firewalls.

II. Features of Vertical Integration Proposals Bearing on Economic Analysis

Six "major proposals" debated within the VI Working Group are listed in the Report. In addition, we previously have made our own proposal. The proposals differ in a number of ways. These differences can be seen by envisioning them as branches of a decision-tree relating to specific dimensions of the decision.

The first set of branches involves the scope of vertical arrangements subject to the rule. This involves the degree of cross-ownership, as measured by the percentage of ownership, the degree of control or influence over competitive decisions, or both. For example, the SW proposal exempts from the rule acquisitions that result in cross-

[7] This is somewhat analogous to the issue of whether to assign to the real estate developer or tenants the right to retain access to the best space. Here, the issue is whether the right to any value deriving from "good domains" should be assigned to the gTLD operator or the first buyer. The effect of the allocation of that property right on consumer welfare is not obvious. On the one hand, the inability to obtain this information can deter registrants from speculating in domains; on the other hand, a gTLD operator who can extract these profits would have the incentive to invest more in the domain, which could in turn create an incentive to create more and better domains. The net effect of the initial assignment of the right to this type of information on consumers is, as with the other potential effects of vertical integration, complex and properly addressed on a case-by-case basis by experts.

ownership of less than 20-25 percent of a vertically related entity. Alternative approaches could choose different criteria for defining sufficient cross-ownership, either the percentage of ownership or indicia of control.

There are other dimensions to defining the scope of any rule limiting vertical integration. For example, it must be determined whether registry infrastructure service providers ("RISPs") should be subject to the cross-ownership restrictions and whether to apply the restrictions solely to cross-ownership or also to vertical contracts.

Assuming that a vertical relationship between a registry and registrar is considered risky enough to warrant further analysis, the second set of branches involves the decision of whether to have a one-size-fits-all (essentially “per se”) rule for all vertical contractual arrangements and structures or whether to evaluate proposals on a case-by-case basis. On the per se branch, there are two choices: (1) prohibiting all vertical integration (per se illegality), or (2) allowing all vertical integration (per se legality). On the case-by-case analysis branch, in which vertical integration will be permitted in some circumstances but not others, further decision criteria must be adopted, and a decision-maker must be identified.

For example, the SW proposal recommends the case-by-case branch and uses market share as an initial screen. If market share falls below a specified threshold, vertical integration is permitted. Alternative proposals could use different market share thresholds. It is difficult to accurately measure market power. Market definition and the evaluation of market power are contentious issues in most antitrust cases and often

require complex economic and econometric analysis. However, market share is a common, albeit imperfect indicator of actual market power.[8]

Under the SW proposal, if the market share of the registry or registrar exceeds the specific threshold, vertical integration is not prohibited. Instead, it is delayed for a certain, specified period of time while it is subjected to further analysis. However, this is not the only approach that could be taken for this set of branches. An alternative approach could prohibit all vertical integration structures that exceed the threshold. Another alternative could subject any vertical arrangements falling below the threshold to further analysis.

The third set of branches of the tree involves the choice of entity to carry out any further analysis that is warranted. The SW proposal refers that analysis to national competition authorities; the application is delayed for a period while the analysis is carried out. An alternative could involve further evaluation that is carried out instead by the ICANN staff or an ICANN committee. This set of branches also can differ according to the default outcome if the competitive authority does not respond; either the application can be rejected or the application can be permitted.

III. Summary and Evaluation of Policy Proposals

The Report refers to six "major proposals" debated within the VI Working Group: JN2, Free Trade, RACK+, CAMv3, DAGv4, and IPC. The Report observes that “no

[8] Registrar market shares could be based either on the percentage of total gTLD registrations under management by the registrar, or it could be based on the percentage of newly created gTLD registrations by the registrar in the last year. For measuring registrar market power, we believe that the percentage of newly created gTLD registrations is a more appropriate measure, because this measure is a more accurate proxy for the potential buy-side market power issues that exist at the registrar level. With respect to registries, we believe that the percentage of total gTLD registrations is a more appropriate measure. These market share calculations should be based on the share of the entire company. We also believe that it is most appropriate to base the calculation of market shares on the total number of gTLD registrations.

consensus has been reached on a proposed model on vertical integration and cross-ownership." We summarize the critical economic characteristics of each of the six major proposals, relative to the Salop-Wright proposal.

A. DAGv4 Proposal

The DAGv4 proposal ("DAGv4") represents a per se prohibition against vertical integration or cross-ownership between registries and registrars, with only limited exceptions. For example, a registrar or an affiliated entity is allowed up to a 2 percent ownership stake in a registry. A registrar or its affiliate may not hold a registry contract, nor may a registry entity control a registrar or its affiliates. Further, registries may not distribute names in any TLD.

B. Free Trade Proposal

The Free Trade proposal is at the other extreme -- per se legality. It would eliminate any and all restrictions on vertical integration and cross-ownership for all registries, registrars, and RISPS in the new TLDs. Under this proposal, an integrated registry-registrar would be able to distribute its own TLD. The Free Trade proposal observes that "setting random percent ownership limits does nothing to mitigate harms and abuse," and that "no harms have been showed to have occurred unmanageably to date, in any namespace, due to lack of vertical integration/ cross-ownership restrictions."[9]

C. Intellectual Property Constituency (IPC) Proposal

The IPC proposal ("IPC") expresses its support for the strict per se prohibition on vertical integration and cross-ownership endorsed by the ICANN Board in the DAGv4

[9] Initial Report, at 39.

proposal. IPC, however, carves out certain exceptions to this prohibition for branded TLDs. The exceptions proposed by IPC would, generally, allow for vertical integration only in instances where the TLD is owned and operated by a trademark holder who is also the registered name holder of all of the second-level domain names in the TLD, or whose trademark licensees are the registered name holders.

D. JN2 Proposal

The JN2 proposal ("JN2") would permit cross-ownership between registries and registrars that meet both of the following two cross-ownership thresholds: (1) less than 15 percent equity stake, or (2) lack of "control," where control is defined as "the possession, indirect or direct, of the power to direct or cause the direction of the management and policies of a person or entity, whether through the ownership of voting or debt securities, by contract, or otherwise."[10] All cross-ownership between Registry operators (and their affiliates) and registrars that serve as an ICANN-accredited registrar in that TLD that exceed either one of these thresholds would be prohibited, unless it satisfies one of the following three exceptions: (1) single-registrant TLDs, (2) community applicants (maintaining up to 30,000 registrations), and (3) an orphan registry operator (a registry operator who cannot attract distribution from existing registrars may register up to 30,000 domain names). Where cross-ownership is permitted, registry operators are prohibited from distributing names within their own TLD. Registrars would be permitted to be registry operators, but only within a TLD for which they are not an operator.

[10] Vertical Integration PDP Working Group Initial Report, at 35.

Under JN2, RISPs[11] will be bound by restrictions on vertical integration only if they "are Affiliates with [the] Registry Operator" or "otherwise control the pricing, policies or selection of registrars for that TLD."[12]

JN2 contemplates limited exceptions for single-registrant TLDs, community TLDs, and orphan TLDs. In these cases JN2 also states that "ICANN may consult with the relevant competition authority at its discretion when reviewing any of these requests for approval" and, when it does so, "should use a 'public interest' standard." "Public interest" is not defined in the JN2 proposal. Nor does it explain what criteria ICANN should evaluate.

E. RACK+ Proposal

Like JN2, The RACK+ proposal ("RACK+") would permit vertical integration and cross-ownership up to 15 percent. RACK+ also recommends ownership caps and limits on vertical integration that result in corporate control.[13] RACK+ is more restrictive than JN2 by eliminating exceptions for single-registrant, community, and orphan TLDs. RACK+ observes that the potential benefit of such a limit is that it "avoids creating ownership positions that provide incentives for registries and registrars alike to

[11] JN2 refers to RISPs as "back-end service providers." For the sake of continuity, we will use the term RISPs for our analysis.

[12] *Id.* at 37. The JN2 Proposal defines "control" as "the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person or entity, whether through the ownership of voting or debt securities, by contract, or otherwise." It goes on to explain, "as used in this definition, the term 'control' means the possession of beneficial ownership of more than fifteen percent (15%) of the interests entitled to vote for the election of, or serve as, the board of directors or similar managing authority of the entity." *Id*. at 35.

[13] RACK+ adopts the same the definition of "control" as the JN2 proposal. Control is inferred from either a 15 percent equity stake or a 15 percent share of voting interests. *Id*. at 47.

discriminate against unaffiliated competitors."[14] RACK+ specifically notes that its proposal is "intended to minimize the possibility of abuse of registry data through structural separation." RACK+ does not consider "less restrictive" alternatives such as internal firewalls for dealing with the potential for abuse of sensitive competitive information by vertically integrated registrar/registries.

F. CAMv3 Proposal

The CAMv3 ("Competition Authority Model") proposal is similar to SW. It establishes a multi-step process for approval of a registry (registrar) request to acquire any ownership interest in a registrar (registry). The multi-step process would apply to acquisitions of an ownership interest but not to vertical contracts. CAMv3 has three essential components. The first is the establishment of a "Competition/Consumer Evaluation Standing Panel" ("CESP"), which would include "economics, law, consumer protection and policy experts from each of the five ICANN geographical regions."[15] CESP would be responsible for evaluating all applications by registries and registrars seeking to acquire an ownership interest in a "different type of Registration Authority."[16] CESP would conduct a "quick look" analysis to determine whether any competition or misuse of information issues are present. If the CESP determines that there are no such issues, the vertical integration would be permitted in the absence of other problems with the gTLD application.

If CESP determines there are competition or consumer protection issues, that determination triggers a referral process, whereby ICANN would "refer the matter to the

[14] *Id.* at 46.

[15] *Id.* at 50.

[16] *Id*. at 49.

appropriate national competition and/or consumer protection agencies" along with the CESP report describing the competitive concerns. ICANN would withhold approval of the application for 45 days to allow for competition agency review. If the competition agency indicates that the vertical integration might violate its competition or consumer protection laws, CAMv3 would require ICANN to place the application on hold for another 60 days after the deadline of any information requests the competition agencies have made upon the applicants.

G. Summary of Vertical Integration PDP Working Report

The following chart summarizes the key features of the various proposals according to our decision tree elements:

PROPOSAL	SCOPE OF THE RULE	PER SE OR CASE-BY-CASE	WHO CONDUCTS ANALYSIS	SUMMARY
DAGv4	Beneficial ownership > 2%	Per se prohibition of cross-ownership and integration	ICANN	Per se illegality
IPC	Beneficial ownership > 2% with limited exceptions for branded gTLDS	Per se prohibition of cross-ownership and integration; conditions for brand exceptions	ICANN	Per se illegality with limited safe harbor
RACK+	Cross-ownership for <15% and without control exempted; registries may not distribute names within own TLD	Per se prohibition above the relevant threshold	ICANN	Per se illegality with safe harbor
JN2	Cross-ownership for <15% and without control exempted; registries may not distribute names within own TLD; exceptions allowed	Per se prohibition above the relevant threshold ; exceptions evaluated on “public interest” standard	ICANN	Per se illegality with safe harbor
CAMv3	All vertical cross-ownership but not vertical contracts	Case by case; Referral to competition agency upon determination by expert panel	Competition authority; affirmative action required for approval	Permissible only if competition authority explicitly approves
SW	All vertical arrangements	Case by case; Referral to competition agency if market share above specified threshold (40-60%)	Competition authority; affirmative action required for rejection	Permissible unless competition authority explicitly disapproves

IV. Commentary: Why We Prefer the Salop-Wright Proposal

It is not a surprise that we prefer our own proposed rule. In this section, we explain why. We also discuss some potential alterations that might be considered in light of the concerns of the other rules.

While the Free Trade proposal avoids the over-inclusiveness problems of some of the other proposals, we believe that it does not adequately address the possibility of competitive harms. The fact that vertical integration and vertical contracts between registries and registrars can create both competitive harms and benefits suggests that per se rules will not be in registrants' interests.

The DAGv4 and IPC proposals involve per se illegality. As such, we believe that they are over-inclusive. While these bright-line rules are less costly to administer than fact-intensive standards, they inevitably will sacrifice consumer benefits. They will prohibit more pro-consumer vertical integration than is in the interest of registrants. In contrast, the SW and CAMv3 proposals are case-by-case rules that cover all vertical contracts, not just cross-ownership. As a result, they will lead to fewer mistakes. Case-by-case analysis is more difficult and takes more time, but we believe that this additional work is warranted in order to increase competition for the benefits of registrants. This approach may harm certain competitors, but in our view, the higher welfare of registrants should take priority.

In our view, JN2 and RACK+ also do not go far enough to protect the registrants' interests in the competitive benefits of vertical integration and cross-ownership between registries and registrars. None of these other proposals is conditioned on the presence of market power at the registry or registrar level. Because competitive harms can be

generated by contract without integration, these proposals do little if anything to prevent the competitive harms with which they express concern.

JN2 severely restricts both the conditions and extent of integration along several dimensions, relative to SW. Most importantly, the JN2 restrictions would apply to all registries and registrars, regardless of market share. In this way, it cuts more broadly. In contrast, JN2 restrictions reach only cross-ownership, not also vertical contracts. JN2 also effectively delegates the responsibility for competition policy analysis and decisions to ICANN rather than to an expert antitrust agency.

RACK+ also is too restrictive towards the risk of misuse of competitive information. That problem perhaps could be remedied with firewalls, which could address the issue without restricting vertical integration and giving up its competitive benefits. To the extent that ICANN believes that misuse of information is a serious concern, the SW proposal could be modified to allow ICANN to require, as a condition of approval, that RISPs impose internal firewalls between data in a registry and its affiliated registrars.

The SW and CAMv3 proposals are most similar, but they differ in several important ways. First, the CAMv3 referral standard relies on subjective criteria that require the CESP to make determinations, whereas the SW referral standard depends only on market share. The CAMv3 proposal uses a subjective and ambiguous "public interest" standard, which increases the likelihood that more applications that do not pose any competitive threat to registrants and are likely to generate benefits will be referred and ultimately rejected. In contrast, economic theory and empirical evidence suggests that that market power is the best single indicator of whether vertical

integration is capable of generating competitive harms. SW is consistent with the economics of vertical integration, and therefore, would permit vertical integration and cross-ownership for registries and registrars that are unlikely to have market power and impose restrictions or conditions on vertical integration between registries and registrars when market power is present. Our market share screen, similar to that employed in both U.S. and European antitrust law, would avoid much of the over-inclusiveness of the alternative proposals by providing a safe harbor for acquisitions below the relevant threshold.[17]

Second, the default presumption of CAMv3 is that vertical integration is *not* allowed unless and until the competition agency approves the proposed integration, whereas SW applies the opposite default presumption, which we believe is the more appropriate default in order to protect registrants' interests in vigorous competition.[18] Third, CAMv3 also is unclear as to precisely what steps would suffice to deviate from the default rejection if a competition agency does not respond. This suggests that many applications likely would be rejected through operation of the default despite the fact that they may not trigger competition concerns. All in all, we believe that the CAMv3 default rule will prohibit more pro-consumer vertical integration than is in the interest of registrants.

* * *

[17] We have proposed measuring a registry's market share as its share of total registrations across TLDs and a registrar's market share as its share of "new creates" within a TLD.

[18] In other words, applicants are “guilty until proven innocent” In CAMv3 and the opposite in SW.

In sum, we believe that SW best grapples with the complexities of any competition policy concerning vertical integration and balances registrants' interests in benefiting from the likely competitive virtues of these arrangements while retaining protection against their possible harms. We have attempted to protect competition and registrant welfare, rather than protecting incumbent competitors. We have attempted to avoid the over-and under-inclusiveness of the per se rules. Relative to the other rules, we rely on what we view as reasonable levels of cross-ownership and market share as objective measures that ICANN can use. We also recommend that ICANN rely on the expertise and experience of the national competition authorities rather than attempting to replicate that expertise itself, possibly on an ad hoc basis.

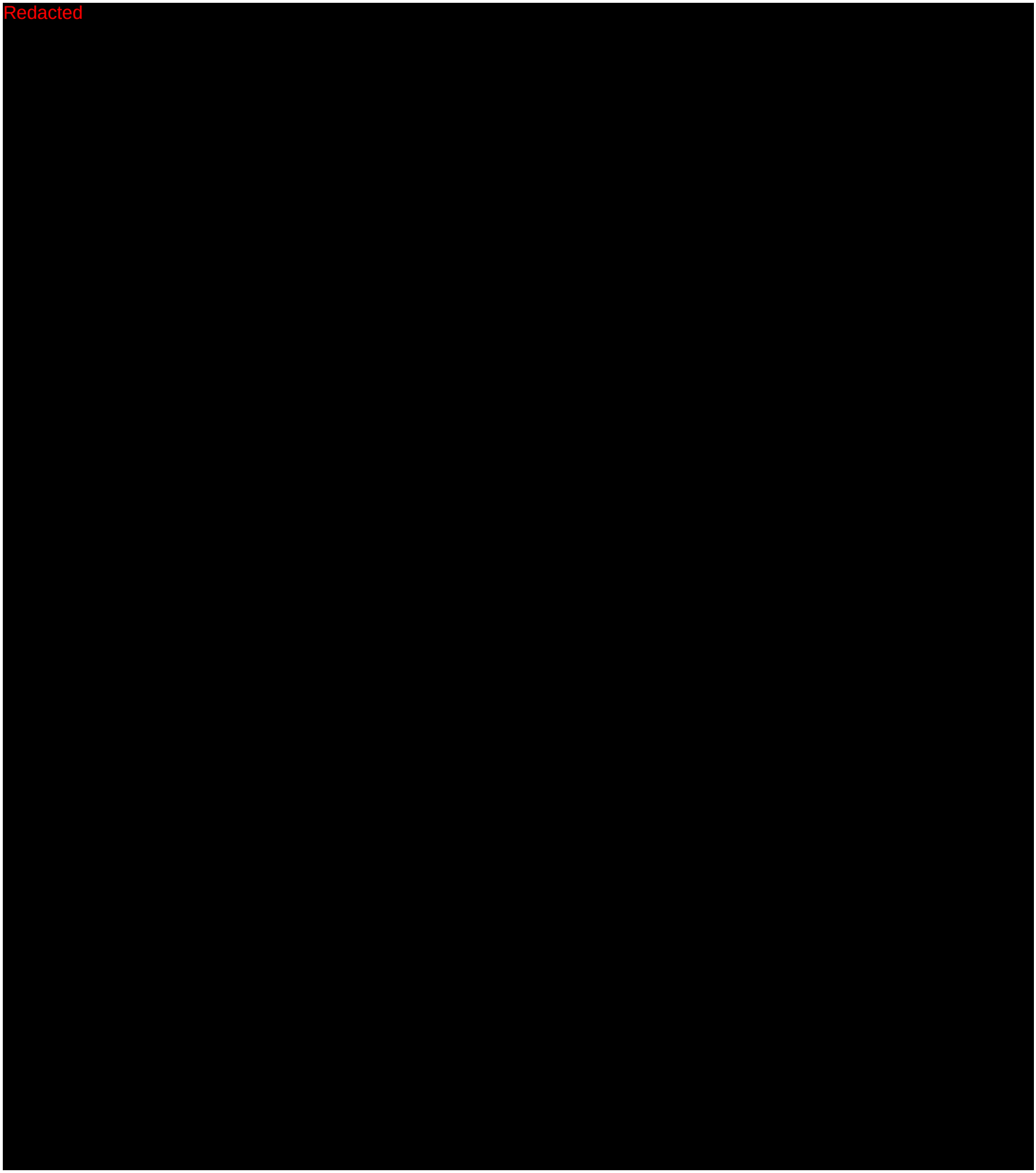
However, the other proposals suggest several ways in which ICANN might modify the SW proposal. First, ICANN also could make the SW proposal more restrictive by choosing lower market share and/or cross-ownership thresholds, or by adding a measure of control by the acquiring firm. While we do not think that these changes are necessary, we believe that these modifications would allow ICANN to achieve its goals without altering the basic structure of our proposal. Second, if ICANN believes that SW proposal does not sufficiently address the concerns of misuse of sensitive information, we suggest that ICANN require integrated entities to maintain firewalls. We believe that this less restrictive alternative can deal with the issue, rather than restricting vertical integration solely to deal with that concern. Third, if ICANN believes that the SW proposal creates too much risk that registrars or registries to achieve market power, it could include a backstop provision. That provision could

require registrars or registries that achieve substantial market power to divest their ownership of entities at the other level.

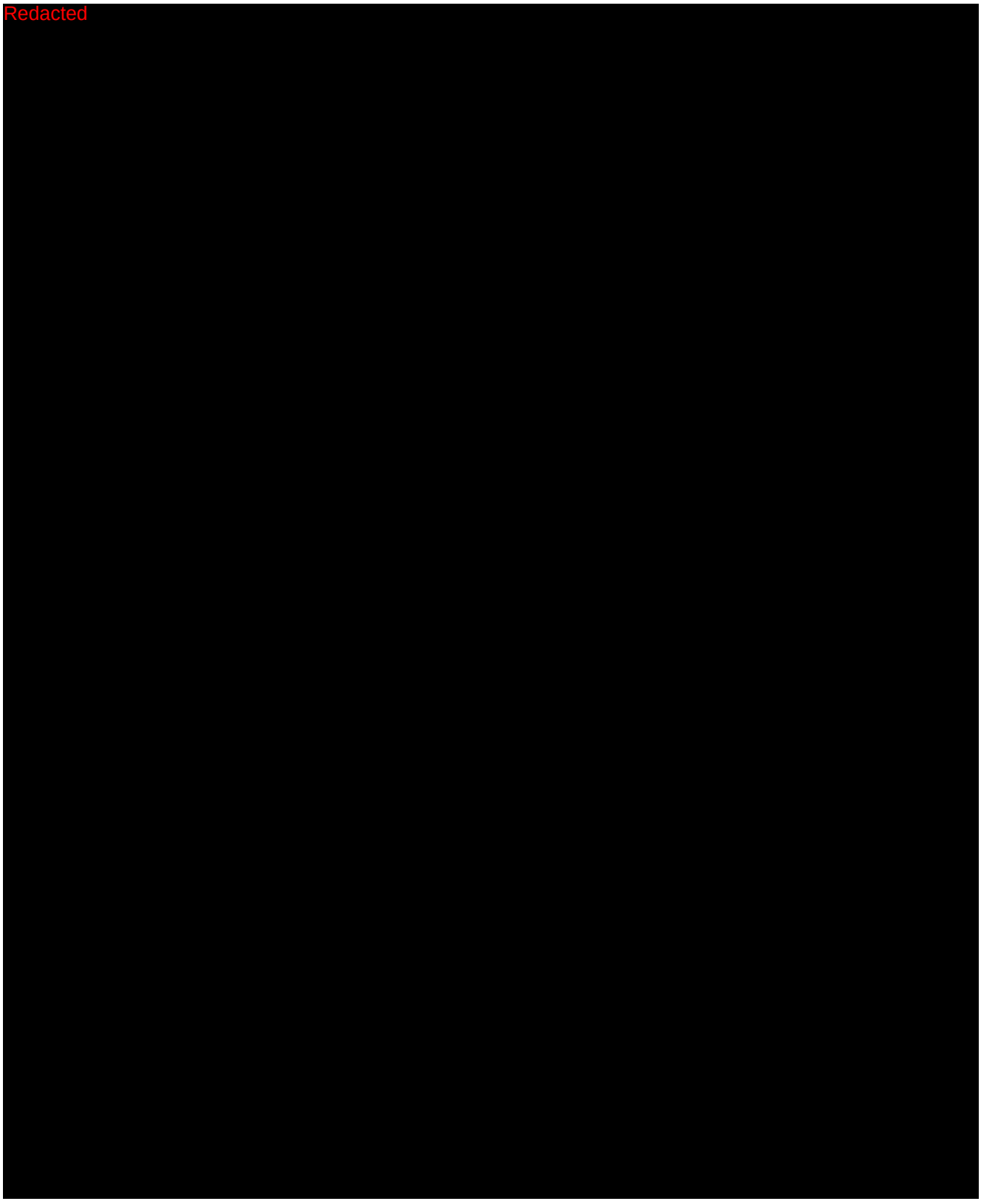
Exhibit B:

Redacted

Redacted



Redacted



Redacted