Report of Public Comments

Title:	Mitigating the Risk of DNS Namespace Collisions
Publication Date:	26 February 2014
Prepared By:	ICANN

Comment Period:	
Comment Open Date:	26 February 2014
Comment Close Date:	31 March 2014
Reply Close Date:	21 April 2014
Time (UTC):	23:59 UTC

Important Information Links
Announcement
Public Comment Box
View Comments Submitted
Report of Public Comments

Staff Contact:	Francisco Arias	**Email:**	francisco.arias@icann.org

Section I: General Overview and Next Steps

The public comment forum received 28 comments in the period from a full range of sources, including applicants and those affiliated with applicants, corporations not directly affiliated with applicants, individual technology experts, and various DNS related industry organizations. In general, contentious issues were relatively balanced with comments reflective of opinions on all sides of the issues.

Some key themes expressed in the comments included:

- Concerns related to the current use of the Second Level Domain (SLD) Block Lists and the Alternate Path to Delegation in general
- Concern that the proposed 120 day "controlled interruption" period is too long/not justified
- Both support and concern regarding the use of 127.0.53.53 as the "controlled interruption" IP address
- Debate relating to the pros and cons of "honeypot" vs. Loopback (127/8) approaches
- Both support and concern regarding the "clear and present danger to human life" threshold
- Questions/comments/suggestions regarding potential implementation details and timelines
- Concerns about availability of the full report ("Phase Two")
- Comments/suggestions relating to .corp, .home, and .mail
- Issues related to brand-oriented applications including SLD block list issues, interaction with Sunrise periods, and general Intellectual Property issues
- Ideas for accelerating closure of the collisions issue in general
- Comments concerning business, competitive, and commercial issues
- Comments concerning the use of DNS wildcard names
- The need for outreach to ISPs

The next steps will be for JAS to provide a final report incorporating the input that will be published and for ICANN to provide a proposal based on the input from the community for the ICANN Board New gTLD Program Committee (NGPC) consideration.

Section II: Contributors

At the time this report was prepared, a total of 28 community submissions had been posted to the Forum. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III), such citations will reference the contributor's initials.

Organizations and Groups:

Name	Submitted by	Initials
Alexander Siffrin	dotSaarland GmbH	AS
Jason Fesler	Yahoo	JF
Martin Levy	CloudFlare	ML
Limei Liu	CONAC	LL
Patrick Flaherty	Verizon	PF
Pierre Bonis	Afnic	PB
Ashley Roberts	Valideus Ltd	AR
Stephanie Duchesneau	FairWinds Partners	SD
Statton Hammock	United TLD	SH
Mason Cole	Donuts	MC
Rubens Kuhl	NTAG	RK
Burt Kaliski	Verisign	BK
Bret Fausett	Uniregistry	BF
Sarah Falvey	Google	SF
Donna Austin	ARI Registry Services	DA
Christian Dawson	ISPCP	CD
Yi Ding	CNNIC	YD
Claudia Höhne	ESMT European School of Management and Technology	CH
Keith Mitchell	DNS-OARC	KM
Andrew Merriam	NTAG	AM
Jonathan Frost	.Club Domains	JF
Steve DelBianco	BC	SD

Individuals:

Name	**Affiliation (if provided)**	**Initials**
Aaron Beck	None Provided	AB
Andrew Gardner	None Provided	AG

Section III: Summary of Comments

General Disclaimer: This section is intended to broadly and comprehensively summarize the comments submitted to this Forum, but not to address every specific position stated by each contributor. Staff recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).

Overall

LL: The report of Mitigating the Risk of DNS Namespace Collisions correctly points out that DNS namespace collision is a pervasive occurrence, which will not put the security and stability of the global Internet DNS itself at risk…

PB: Afnic commends ICANN dedication to the security and stability of the Internet, but wonders why, given the fact name collisions are reported to be a well-known threat and the blocked names list has been published since November 2013, there is still a need to block all these names for a period of 120 days after delegation of the TLD.

AS: …we [dotSaarland] appreciate the recommendations of the study as a solution that allows for an activation of the affected strings in the DNS while providing a clearer, more targeted approach to identify actual risks as opposed to a blanket prohibition of all potential, but probably non-existing risk.

SD: We [FairWinds Partners] write to express our support for the proposal, insofar as it allows Registry Operators to fully use their gTLDs.

MC: Notwithstanding some exceptions discussed below, Donuts agrees with and supports the JAS recommendations, and encourages their expeditious approval and implementation.

MC: There is no empirical or even anecdotal evidence that name collisions are a problem necessitating the extensive restrictions, let alone those placed on new gTLD operators only… We [Donuts] further reaffirm our position that because name collisions pose no real threat to life or Internet stability, name collision mitigation is an unnecessary burden unfairly placed on new gTLD registry operators as a method to limit competition in the domain space.

YD: CNNIC appreciate for the new name collision mitigation report by JAS Global Advisors, especially support the Recommendations 6 and 7 which registry should set controlled interruption zone or A & SRV resource record on Blocked 2LD.

DA: ARI Registry Services welcomes the study report by JAS Global Advisors "Mitigating the Risk of DNS Namespace Collisions". The report is sound and for the most part, ARI Registry Services supports the recommendations, with the exception of Recommendations 6 and 7 which call for a 120 day controlled interruption periods.

RK: Notably, we [NTAG] wholeheartedly agree with the first finding of the report: "We [JAS] do not find that the addition of new Top Level Domains (TLDs) fundamentally or significantly increases or changes the risks associated with DNS namespace collisions". This conclusion is consistent with the experience of registries that introduced new gTLDs in the 2000 and 2004 rounds, the introduction of IDN ccTLDs, the delegations of recent ccTLDs such as .SX, and the experience of community members that have run end-user networks.

JF: I appreciate the analysis and recommendations put forth by JAS Global Analysis in the "Mitigating the Risk of DNS Namespace Collisions" phase 1 report. In general, I concur with the findings and recommendations.

BK: …the security, stability and resiliency of the DNS is one of ICANN's priorities, and rightly so. The Phase One Report confirms, as others have previously concluded, that these properties are not at risk due to name collisions related to new gTLDs.

BK: JAS Global Advisors has done a credible job diagnosing the symptoms (even if the full diagnosis remains doctor-patient confidential at the moment), and as recommended a novel treatment.

SF: In general, JAS Advisors has done a thorough and insightful job of analyzing potential collisions due to the delegation of new top-level domains (TLD), and their proposed approach of adopting a controlled interruption period seems to be an appropriate precaution as part of the process of introducing new gTLDs. Notably, the controlled interruption framework should be superior at detecting problems and provides a better balance between the usability of new gTLDs and the protection of existing computer systems and technical process, compared to the blocklist approach employed in the Alternative Path to Delegation.

Length of Controlled Interruption Period

MC: There is no data supporting a 120-day delay. This number was based on the 120 days from contracting provided to certificate authorities to revoke certificates. If there were to be any delay at all, domain name lifecycle standard of a range of 45-90 days should be used.

SF: …we [Google] see no reason for a controlled interruption period longer than 45 days, which should be adequate to detect any serious problems caused as a result of the TLD's delegation.

DA: The report provides no valid reason for requiring the 120 day controlled interruption period except that it is consistent with the benchmark set by 120 day CA Revocation period, which the report acknowledges is overly conservative… Given that JAS has acknowledged that the 120 day period is overly conservative and that quarterly cycles are 90 days, there does not appear to be solid justification for the 120 day controlled interruption periods, rather it seems that the 120 day period is arbitrary at best and not able to be substantiated in any legitimate way. We would ask that consideration be given to reducing the controlled interruption period to 38 days based on the following rationale…

BK: As far as the length of the controlled interruption period, the rationale for 120 days based on the amount of time it may take a user or system administrator to detect the break and then fix it - potentially across a large corporate network - seems quite reasonable as starting point for an untested technique. With more operational experience…it may be possible to justify a shorter period.

RK: The 120 day period is not sufficiently supported by data or analysis, and does not mirror similar processes either in the domain name space or across other relevant industries…In fact, a similar need in the telecommunication industry typically warrants the use of a transition period lasting up to 60 days, and the operational experience of applicants suggested that no longer than 45 days would be required for DNS infrastructure.

YD: we have read the comment from ARI Registry, which supposed to reduce the 120 day period in recommendation 6 and 7 to 38 days, we consider the reason described in their comment extremely rational, and we totally support the 38- days controlled interruption suggestion.

PF: We query if this 120-day period is sufficient both in time and in process to permit the affected end user to identify – much less remediate – collisions.

PB: The reason for the 120-day period for controlled interruption is not clearly explained in the report. If a registry is capable of demonstrating to ICANN that it has mitigated the name collision, the concerned SLD should be activated immediately. Contractual obligation vis-a-vis the registry and the SLD owner sometimes may not allow the registry to block the SLD for 120 days.

SH: United TLD recommends that ICANN drop the 120 day period to 60 days. While the extra 30 days doesn't seem like much compared to the magnitude of delays the New gTLD Program has faced, a 60 day period will more closely match a typical 60 day Sunrise Period.

JF: The comments of the NTAG, Donuts, Rightside/United TLD, and Ari Registry Services have thoroughly and competently explained why the 120 day interruption period of Recommendation 7 is excessively conservative. A merely conservative interruption period of 60 days is more than adequate for registries that have already been delegated, because the detrimental effects on public interest must be balanced against the security interest of a longer interruption period. A lengthened interruption period is significantly detrimental to the public interest because it would cause confusion for commercial registrants.

BK: There does appear to be general consensus that the controlled interruption period, if the mitigation measure is adopted, should begin as soon as the registry agreement is executed for a new gTLD, which would allow, quoting NTAG's comments, "for the maximum opportunity for third parties to assess unlikely leakages while minimizing the disruption of the Registry's business model."

Honeypot vs. Loopback

SF: Although the proposal to resolve names to the 127.0.53.53 IP address would likely allow for the detection of problems, we [Google] believe the use of a hosted honeypot as described in SAC62…provides a better opportunity to inform users of impending problems, while at the same time the honeypot gathers information regarding the usage of the TLD.

BK: A loopback address such as 127.0.53.53 is preferable to an internal network address because it's easier for a general user to manage. An external honeypot address should not be used. If controlled interruption is, in principle, a name collision, then controlled interruption with an external honeypot address is a controlled exfiltration – potentially drawing sensitive personal and corporate data to the collection site over an unencrypted path over the Internet.

SD: A carefully designed "honey pot" approach, as suggested by some commenters, might be effective in identifying collisions and measuring effectiveness of mitigation. However, the BC would not support a honeypot approach that could cause release of sensitive information to the honeypot operator.

AM: …although there is no consensus among our [NTAG] membership on where to use unreachable IP address or provisioning an Internet reachable honeypot, in the case that an unreachable address is used, we recommend sticking to 127.0.53.53…Following one comment already in reply to the first one, we see two good reasons for the 127.0.53.53 response: (1) being in the range that minimizes traffic at all levels since it isn't not reaching any destination at the end (2) it is memorable enough that network administrators can easily search for it.

BK: Verisign maintains its position that directing requesters to an internal address during the controlled interruption period is preferable to an external honeypot, because as previously stated, it avoids "controlled exfiltration" where sensitive traffic from an installed system – without the advance consent of the user or system administrator – may be drawn outside the local network.

JF: I believe the potential for information leakage and remote honeypots to far outweigh any risk of local denial of service possibly created by the use of "127.0.53.53" from Linux/Android hosts.

BK: Other stakeholders have expressed reservations about the 127.0.53.53 address itself. These concerns should be evaluated further, as well as the point about the lack of an IPv6 address.

ML: I simply can't get my head around coding into numerous end-point software subsystems the "127.0.53.53" address. The precedence set by this is non-trivial and this act could potentially open up the 127.*.*.* block (and its lack of v6 equivalent block) to all manner of "solutions" to real or artificial problems. While I highly respect the team that thought this solution up; I also respectfully state that it's just not passing the "smell test". Alas I know I'm failing because I can't bring to the table an alternate solution.

CD: One thing we [ISPCP] like about Controlled Interruption via 127.0.53.53 IF it proves effective is that it makes the problem easily identifiable, so that solutions can be found via search engine by sysadmins.

SH: While United TLD recognizes the concerns about privacy and data leakage, we believe that ICANN should seriously consider using a valid public address that points to an informative web page rather than the 127.0.53.53 IP address for A records. We believe that, assuming the public IP only answers Port 80 requests, it would be much more effective to educate end-users than routing them to an internal IP which offers no ready feedback.

LL: Recommendation 7 of the report in specific --"registries publish appropriate A and SRV resource records for the labels in the ICANN 2LD Block List to the TLD's zone with the 127.0.53.53 address for a period of 120 days" is unnecessary and hard to be implemented by CONAC because the users of the blocked SLDs are important government and public interest related organizations, such as the state council, and we could not impair the Chinese users' experience and interests.

YD: …we have a problem about the controlled interruption [IP address] choice. Could we choose to set wildcard on our TLD which is already delegated but haven't offer registration?

PB: RECOMMENDATION 7: As recommended in the discussions in the collisions mailing list for a better visibility, instead of redirection to 127.0.53.53, ICANN should create a public web server which redirects all the name collisions related queries. The redirected query of course should be stripped of all sensitive data.

Clear and Present Danger to Human Life

SD: The BC notes that systemically significant dangers to the business and financial sectors of the global economy might also merit the use of emergency measures. And if any enterprise were to demonstrate how collisions would endanger their financial survival, that should also merit emergency response.

BK: [Relating to JAS Recommendation 3]: The rationale makes sense, and it also makes sense that this will be one of the more contentious recommendations.

PF: Clear and present danger to human life draws an arbitrary line unnecessarily high and fails to take into consideration what happens if significant financial and other harm results for global businesses and end users.

RK: We [NTAG] agree that the bar for invoking removal of DNS labels should be established as clear and present danger to human life (C&PDHL) instead of just "harm".

SH: United TLD agrees with the study's recommendations that emergency response options should only be considered in cases where there is a clear and present danger to human life, rather than just "harm" and also supports the conclusion that de-delegation is not a valid response even in such case.

Phase One and Phase Two Reports

PF: Until a more comprehensive version of the report is made publically available, we [Verizon] can only provide preliminary comments.

JF: We [.Club Domains] join the NTAG in opposing Verisign's suggestion that an additional comment period is necessary before implementing JAS Advisors' findings; doing so would be an extremely inefficient use of resources and inconsistent with the NGPC Resolution of October 7, 2013.

CD: [Comment by ISPCP] We will never have sufficient data to know for certain what will break during delegation. We ought to focus as much of our attention as possible on documentation and outreach. The report states the outreach done to date, and that's a good start. These efforts need to continue to grow over time and cannot end when the full report is issued.

BK: As the Phase One Report is reviewed by the public, it is important to remember…that the report alone is not the name collision management framework ICANN resolved in October 2013 that it would develop. Rather, the report suggests a generic mitigation measure, controlled interruption, to be applied to all new gTLDs (except for the three that are to be blocked entirely). Presumably the framework will be included in the Phase Two Report, now expected in June. But it would be premature for ICANN to act on the Phase One Report and implement its recommendations, before the actual framework that ICANN resolved to develop is available for public review.

BK: Until the Phase Two Report is published, it is not possible to verify if … the analysis leading to the assessment [in the JAS report] is correct.

SD: Because the framework and data supporting the findings and recommendations of the report are still pending release, the BC asks ICANN to reserve final closure on collision-related recommendations and actions until the community has received the full report and has been given the opportunity to review and comment

Issues relating to corp, .home, and .mail

SH: United TLD recommends that a final decision on these strings be postponed until a more comprehensive technical evaluation can be performed and a solution may be developed to allow for these strings to operate in the DNS.

PF: We [Verizon] are pleased that JAS recognized the concerns about the new gTLDs .corp, .home, and mail, and we fully support JAS' recommendation that all three gTLDs be permanently reserved.

RK: We [NTAG] ask that the .home, .corp and .mail decision be addressed in a more comprehensive technical discussion regarding these 3 strings and unapplied-for labels to be possibly used as local DNS spaces.

SF: We [Google] agree that a TLD reserved for internal usage is desirable and encourage ICANN to work with the IETF standards-setting process to establish such a namespace.

BF: We [Uniregistry] strongly disagree with one aspect of the JAS report, which is that .HOME, .CORP and .MAIL should be permanently reserved. One of the primary purposes of the proposed mitigation plan is to educate users about the potential technical issues involved in private namespaces. Contrary to this purpose, permanent reservation of these three TLDs will perpetuate conduct that the rest of the mitigation plan is designed to cure. If these three TLDs present special cases, then ICANN should consider a mitigation period longer than 120 days solely for HOME, CORP and MAIL, but it should not permanently reserve them.

MC: It is premature to preclude altogether the existence of these three gTLDs. Nothing is gained by such an action and preventing an opportunity for study, coordination with the IETF, or other such prudent and reasonable examinations.

BK: Although it may be clear (pending publication of Phase Two Report) that these three applied-for new gTLDs are categorically at higher risk than all the rest, is it also the case that there are no SLDs in all the other applied-for new gTLDs that are of high enough risk to consider blocking indefinitely? The risk doesn't need to be high on average, just for enough installed systems. But without the benefit of the risk criteria Phase Two Report, there's not enough information on which to draw a conclusion.

MC: Donuts disagrees again with comments that recommend these gTLDs be permanently prohibited. ... Donuts agrees with Uniregistry's comment of March 31 ... Again, the ICANN Board is better advised to postpone any decision regarding .HOME, .CORP and .MAIL until the complete report is published, and provide a comment period for not only those strings, but potential other labels that could be used as local DNS spaces.

Issues related to brand-oriented applications including SLD block list issues, interaction with Sunrise periods, and general Intellectual Property issues

SF: We [Google] support the comments filed by Valideus and FairWinds suggesting that all names, which registries were forced to block under their alternative path to delegation plans, be subject to the Sunrise and Trademark Claims services outlined in the gTLD Applicant Guidebook, the Registry Agreement, and the Rights Protection Mechanism Requirements (RPMs).

AR: Upon looking at the SLD Block Lists for .brand applicants it becomes clear that many of the terms are trademarks for the brand's products and services, seemingly generated at the root by the brand itself. It is counterintuitive for a brand to be barred from using names corresponding to its trademarks, for which it was the cause of the root server query, so we would also suggest that ICANN

consider an alternative process for .brand applicants to expedite the release of such trademarked terms for their immediate use

AR: Therefore, in the event already-launched TLDs release names for registration from their SLD Block Lists, we suggest these names should be subject to Sunrise and Trademark Claims.

SD: The requirement to include names on a Registry Operator's SLD block list in the Sunrise Period is imperative to preserving the Sunrise Period's effectiveness in protecting trademark holders' rights.

SD: ...it was made explicit that all names on a Registry Operator's SLD block list would be subject to both the Sunrise Period and the Claims Period requirements... The requirement to include names on a Registry Operator's SLD block list in the Sunrise Period is imperative to preserving the Sunrise Period's effectiveness in protecting trademark holders' rights.

SD: FairWinds requests that Recommendation 7 be revised to include the requirement that all names that are on the SLD block list must have passed through the Sunrise Period before they can be released for registration, as well as the requirement that such names pass through the Claims Period during the first ninety days that they become available to the general public, as well as during any Limited Registration Period they are included in.

CH: We found out that the domain esmt.berlin is on the ICANN Collisions List and we don't understand why. Our institution is called ESMT European School of Management and Technology (located in Berlin)...

SF: We support the comments filed by Valideus and FairWinds suggesting that all names, which registries were forced to block under their alternative path to delegation plans, be subject to the Sunrise and Trademark Claims services outlined in the gTLD Applicant Guidebook, the Registry Agreement, and the Rights Protection Mechanism Requirements (RPMs).

JF: .CLUB Domains Opposes Fairwind Partners' and Google's Recommendation that Alternative Path Block List Names must be subject to a second Sunrise because implementation of a second Sunrise is not practical and ICANN may lack the contractual authority to impose that condition on TLDs that have already signed Registry Agreements.

Use of DNS Wildcards

SH: United TLD also suggests that TLDs that have elected the "alternative path to delegation" also be allowed the option of wildcarding the TLD as a method of controlled interruption. Registries should be able to have both options available. This would effectively eliminate the issues with non-registered zone entries and likely be easier to manage for registry operators that would otherwise face the challenge of either artificially registering thousands of domains or manually adding entries to their zone files.

MC: Forcing registries to wildcard the zone for 120 days from delegation introduces another 30-60 days of delay to market.

RK: We welcome the idea of wildcarding the TLD, but disagree ... request that any wildcarding solution be implemented immediately upon signature ... wildcarding and alternate path to delegation both be allowed to all registries ... some back-end DNS publishing systems used by registries do not support DNSSEC wildcards ... This would require a modified name server, because there is no provision in the standard zone file format for specifying that a response should be returned for all SLDs except those on a defined list, i.e., no "wildcard-with-exclusions" option.

CD: ... every possible second level domain would be delegated by wildcard ... There should be an exception process ... Otherwise, the Controlled Interruption may create risks ...

YD: we would like to choose the wildcard ways, and then open registration after 120 day after wild card setting. Could this choice be available for the "alternative path to delegation" registry?

BK: The complexity of the approaches discussed here should serve as a reminder why the Internet technical community has recommended against the use of wildcards[32]. They're powerful constructions, but they're hard to use correctly, can easily go wrong. Indeed, wildcards head in the same, potentially insecure and unstable direction as dotless domains [33][34], which are disallowed by ICANN [35] (see also the discussion under the fourth comment of [4])

Commercial and competitive issues

MC: gTLD operators that have executed contracts prior to the approval of the JAS plan should be grandfathered—that is, ICANN should honor its contracts with registry operators that include the Alternative Plan right, at an operator's option, to block proscribed second-level terms as a mitigation strategy. Any contracts signed after the approval of the JAS plan would not include such ability

MC: Registries should not be required to pay ICANN fees during the "controlled interruption" period

MC: The name collision issue is creating an uneven competitive landscape…It is abundantly clear that collision exists to a far greater degree in .COM and other legacy TLDs than they do or will in new gTLDs in general. The idea that only new gTLD operators, and not legacy operators, should use mitigation as an educational tool for network operators places yet another burden on new gTLDs that is suspiciously not required for existing TLDs.

DA: New gTLD Applicants have been severely penalized by many elements of the new gTLD implementation process that have imposed delays or changes to the process under which applicants applied…

PF: It appears that JAS recommends pushing much of the responsibility for dealing with the fallout from domain name collisions from ICANN, where the responsibility should reside, to the end user community, including businesses and likely ISPs. We also disagree with JAS' assumption that the experiences of past new gTLDs launches (where a small number of slow and controlled introductions of well-vetted gTLDs) will necessarily mean that there will not be significant incidents of domain name collisions from the introduction of enormous numbers of new gTLDs.

MC: Since opening its first set of new gTLDs for Sunrise last November, Donuts has administered more than 600,000 domain name registrations. There have been no collision problems in any of these gTLDs; given the nature of the attention paid to the collision issue, it's something we carefully monitor… However, since merely the close of the past comment period on this matter, Verisign has accepted more than three million registrations in .COM. It's a demonstrated fact that collision infects the .COM gTLD in an impactful way, yet it and other elements of the community not only refuse to address the existing problem, but insist on imposing mitigation strategies only on competitors and not on incumbents.

SD: We [BC] are also concerned about the suggestion in the Phase One Report and the statements of certain commenters that a large part of the responsibility for identifying, remediating, and contacting the originators of the colliding DNS queries should be passed to the business community and Internet service providers. We have similar concerns about suggestions that ISPs should bear the burden of identifying the originating users of colliding queries and that they should supply query data to third parties for analysis.

BK: If there's any unevenness in the domain name landscape, then, it's a result of the tectonic interruptions that are requiring users, system administrators, network operators, infrastructure providers and platform and application developers across the globe to update their installed systems to accommodate 1400 or more new gTLDs. The parties who rely on the global DNS are the ones whose playing field is out of balance due to the largest operational change to the global DNS in its 30-year history.

The need for outreach to ISPs

PB: ... The list of blocked names published by ICANN in November should allow ICANN engaging, along with its customers (the registries) dialogue with ISPs and systems operators to track the queries made that lead to these lists, determine the sources they are originated from, and inform directly the operators that the TLD is going to be delegated.

SD: We have similar concerns about suggestions that ISPs should bear the burden of identifying the originating users of colliding queries and that they should supply query data to third parties for analysis.

Section IV: Analysis of Comments

General Disclaimer: This section is intended to provide an analysis and evaluation of the comments received along with explanations regarding the basis for any recommendations provided within the analysis.

ICANN thanks the community for their participation in this public comment forum. ICANN is carefully considering the comments and will take them into account in the development of a proposal for moving forward with addressing this issue, which will include additional analysis of these comments and their effect. This summary along with the aforementioned proposal will be provided to the Board New gTLD Program Committee for its consideration.