ICANN 12 OCTOBER 2014 NGPC MEETING
Reference Materials

TABLE OF CONTENTS

Main Agenda

TITLE: **GAC Advice in the Beijing Communiqué regarding Category 2 Safeguards – Exclusive Registry Access**

Options for Consideration of GAC Category 2 Safeguard advice

A - Prohibit Exclusive Generic TLDs	
Pro	**Con**
Will satisfy community members that think ICANN should prohibit Exclusive Generic TLDs	Inconsistent with GNSO position
Simple	Inconsistent with AGB
	Arguably inconsistent with GAC Advice; may require GAC consultation

B - Reject GAC Advice **Permit Exclusive Generic TLDs**	
Pro	**Con**
Consistent with GNSO position	Will dissatisfy community members that think ICANN should prohibit Exclusive Generic TLDs
Consistent with AGB	May lead existing registry operators to ask for contract amendment to be Exclusive Generic
Consistent with view that ICANN should adhere to its remit and not regulate business models	Will require GAC consultation

C – Public Comment - Framework to Evaluate Public Interest Goals	
Pro	**Con**
Seeks implementation direction from the community, potentially including the GAC	Public comments may not be able to provide additional clarity to assist implementation
	May be seen as unreasonable delay at this juncture
	Not clear who would ultimately be responsible to evaluate the public interest goals submitted

D - Accept GAC Advice Implement Advice by Requesting Voluntary PIC	
Pro	**Con**
Consistent with treatment of other GAC Advice	Will dissatisfy community members that think ICANN should prohibit Exclusive Generic TLDs
Publication of PICs provides an opportunity for the community to offer feedback on the proposed PICs	May lead existing registry operators to ask for contract amendment to be Exclusive Generic
PICs become contractually binding obligation in the Registry Agreement	Enforcement of PICs may extend ICANN beyond remit

REFERENCE MATERIALS - NGPC PAPER NO. 2014.10.12.NG2a-Attachment B

TITLE: GAC Advice in the Beijing Communiqué regarding Category 2 Safeguards – Exclusive Registry Access

Discussion of Exclusive Registry Access and Generic Strings

Staff believes there is considerable confusion among the community and various constituents regarding what the GAC advice and the New gTLD Registry Agreement actually say about generic strings.

In discussing this topic, many people use the terms "open generics" and "closed generics." Those terms do not appear in GAC's Beijing advice nor do they appear in the New gTLD Registry Agreement. The more appropriate terminology, consistent with the GAC advice and the revisions to the New gTLD Registry Agreement implemented by the NGPC, is to distinguish between "exclusive" and "non-exclusive" registry access.

Exclusive Registry Access

When ICANN launched the New gTLD program, one of ICANN's stated goals was to promote diversity. Applicants responded to that call with a variety of business models. Although some people talk as though there is a binary choice here – either a TLD is completely open and domain names are available to any and all registrants on a first come first served basis, or it is completely closed and domain names are only open to the Registry Operator itself, our applicants recognized that there is a broad continuum between those two models. Some applicants said they do intend to operate in a completely closed manner and only sell domain names to the Registry Operator itself, and some of those applicants suggested they only expect to register a few dozen domain names per year. Other applicants suggested they will operate largely on what some would call an open model – that anyone could register a domain name in the TLD either on a first come first served basis or with other business models permitting registrations of certain names at premium prices.

However, a large number of applicants were somewhere in the middle. Their vision and business model for the TLD calls for registration rules that limit registrations in a variety of ways. Community applications are an obvious example, but there are many others. Applicants for various city names made it clear that registrants would have to show some connection to the city. Even before any GAC advice, some applicants for strings associated with certain professions made it clear that they intended for registrants to be limited to those licensed in the profession. Some applicants made it clear that their registration policies would be limited in ways designed to protect the rights of intellectual property owners rather than being completely open. Nothing in the Applicant Guidebook limited applicants from electing a range of different registration policies consistent with their own business models.

In the Beijing Communiqué, the GAC provided the following advice:

> *For strings representing generic terms, exclusive registry access should serve a public interest goal.*

It is important to recognize two things about this advice. First, the advice does not use either the term "open" or "closed" with respect to generic TLDs. It refers instead to "exclusive registry access." Second, the GAC did not advise that exclusive registry access generic TLDs should not be delegated; it said instead that those TLDs should serve "a public interest goal."

In response to that GAC advice, more than a year ago, on 23 April 2013, ICANN initiated a public comment forum to solicit the community's input on how the NGPC should address GAC advice. The NGPC met on 8 and 18 May and 4, 11 and 18 June 2013 to consider a plan for responding to the GAC's advice on the New gTLD Program, including the Category 2 Safeguard Advice. On 25 June 2013, the NGPC directed staff to make appropriate changes to the final draft of the New gTLD Registry Agreement to implement the GAC's Category 2 Safeguard Advice for applicants not seeking to impose exclusive registry access, and directed staff to defer moving forward with the contracting process for applicants seeking to impose exclusive registry access for "generic strings" to a single person or entity and/or that person's or entity's Affiliates (as defined in Section 2.9(c) of the Registry Agreement), pending a dialogue with the GAC.

The NGPC Resolutions and the changes to the New gTLD Registry Agreement implementing GAC Category 2 Safeguards do not use either the term "open generic" or "closed generic." Consistent with the GAC advice itself, which referred to exclusive registry access, the changes to the New gTLD Registry Agreement provide that a Registry Operator of a generic string TLD "may not impose eligibility criteria for registering names in the TLD that limit registrations exclusively to a single person or entity and/or that person's or entity's "Affiliates." This was included in Specification 11, Public Interest Commitments, making it an enforceable commitment for which ICANN can pursue compliance actions if the Registry Operator breaches this commitment. Note that the implementation of GAC Category 2 Safeguard advice on this issue did not say that a Registry Operator of a generic string had to have completely open registration policies and register domains to any and all registrants. It said instead that a Registry Operator of a generic string could not limit registrations exclusively to a single person or entity and that person's or entity's Affiliates.

Generic Strings

There is also some confusion about what constitutes a "generic string." A "Generic String" means a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others."

Merely because a word has a generic dictionary meaning does not mean it is used in a generic way. When a word or term is used as the common dictionary name for the goods or services it describes, the word is generic. If the word "sushi" is used to identify the Japanese food sushi (i.e., vinegared rice with raw fish), the term is used generically. However, if a business uses the term SUSHI as a brand to identify goods or services unrelated to the food sushi, that would not be a generic use of the term. So a SUSHI brand line of clothing, or a SUSHI brand automobile, or a SUSHI brand photocopying service, would not be a generic use of the term sushi. In those examples, a trademark lawyer would describe the mark as an "arbitrary" trademark, not a "generic" trademark. An arbitrary mark has a common dictionary meaning that has no relation to

the goods or services to which it is applied. In those cases, the selection of the word SUSHI as a brand name for an automobile is arbitrary, for branding purposes; the word does not mean automobile and does not describe any characteristics of an automobile.

If an applicant applies for the TLD string "sushi" and it is in the business of operating restaurants that serve sushi, that would be a Generic String that describes the general class of goods or things comprising sushi. However, if an applicant applies for the TLD string "sushi," and applicant's business is marketing and selling SUSHI brand clothing or a SUSHI brand automobile or a SUSHI brand photocopying service, that would not be a Generic String. In those cases, SUSHI would not be used to denominate the class of food known as sushi, but would instead be used to distinguish SUSHI brand clothing or SUSHI brand automobiles or SUSHI brand photocopying services from other brands of clothing or automobiles or photocopying services.

NGPC Actions to Address the GAC's Category 2 Safeguard Advice

On 19 August 2013, ICANN inquired as to whether the applicants of the 186 applications identified by the GAC as generic strings plan to operate the applied-for TLDs as exclusive access registries as defined in the New gTLD Agreement. As of 29 September 2014, applicants of 10 applications continue to indicate that the applied-for TLDs will be operated as exclusive access registries. ICANN has moved forward with signing Registry Agreements with applicants who indicated that they do not intend to operate the applied for TLDs as exclusive access registries. The question now remaining is what to do about the 10 applicants who maintain that they do want to operate generic strings on an exclusive access basis.

Submitted by: Jamie Hedlund

Position: Vice President, Strategic Programs, Global Domains Division

Date Noted: 29 September 2014

Email: jamie.hedlund@icann.org

REFERENCE MATERIALS – NGPC PAPER NO. 2014.10.12.NG2b

TITLE: **GAC Advice Regarding Protections for the Red Cross and Red Crescent – London Communiqué**

Process for Consultations between the ICANN Board of Directors ("Board") and the Governmental Advisory Committee ("GAC"), including those required pursuant to Article XI Section 2.1.j of the ICANN Bylaws

Process:

Step 1: Upon receipt of GAC advice (and prior to communicating its final decision), the Board will provide a written response to the GAC indicating:

- whether it has any questions or concerns regarding such advice;
- whether it would benefit from additional information regarding the basis for the GAC's advice;
- and a preliminary indication of whether the Board intends to take such advice into account.

The Board's response will be subject of an exchange between the Board and the GAC.

Step 2: In the event that the Board determines, through a preliminary or interim recommendation or decision, to take an action that is not consistent with GAC advice, the ensuing consultations will be considered "Bylaws Consultations". The Board will provide written notice to the GAC (the "Board Notice") stating, in reasonable detail, the GAC advice the Board determines not to follow, and the reasons why such GAC advice may not be followed. The GAC will be afforded a reasonable period of time to review the Board's Notice and explanation, and to assess whether there are additional elements of GAC advice that it believes have been rejected by the Board.

Step 3: As soon as possible after the Board Notice is issued (or within such time as otherwise agreed), the Chair of the GAC and the Chair of the Board will confer as to an

appropriate time and agenda for a meeting between the GAC and the Board (the "Bylaws Consultation"). It is intended that all issues related to the meeting are identified and agreed upon between the GAC and Board prior to the consultation.

Step 4: Within a timeline agreed to by the GAC Chair and Board Chair, the GAC and/or the Board may prepare written documents setting forth their respective positions on the intended Board action for presentation at the Bylaws Consultation. Subject to the agreement to publish documents, such documents should be communicated and will be published at least two (2) weeks prior to the Bylaws Consultation meeting. Where practicable, all communications and notices provided by the Board or GAC shall be posted to ICANN's website. In addition, a written transcript of the Bylaws Consultation meeting shall be posted to ICANN's website.

Step 5: During the Bylaws Consultation meeting, the GAC and the Board will each seek, in good faith and in a timely and efficient manner, to find a mutually acceptable solution to the conflict between the possible Board action and the GAC advice, including by proposing compromise positions with respect to the intended Board action, if feasible and appropriate.

Step 6: After the conclusion of the Bylaws Consultation, the Board will determine whether to reaffirm or reverse the intended Board action, or take mitigating action.

If the Board determines to reverse the intended Board action or take mitigating action based on GAC advice and the outcome of the Bylaws Consultation, the Board may as appropriate: (i) implement any compromise action proposed by or agreed with the GAC during the Bylaws Consultation, in either case without further GAC consultation; or (ii) formally reverse the Board's preliminary or interim decision. The Board's final determination will be communicated to the GAC, providing the GAC an opportunity to comment and/or to raise other issues raised anew by the Board's decision and therefore not addressed in the consultation.

As a general rule, the Bylaws Consultation process should conclude within six months. The GAC and the Board can agree to a different time limit when necessary, taking into account the complexity of the issue and the scope of difference between the GAC and the Board's positions. Either the GAC or Board may initiate a request for expansion of the six-month time limit by providing a written request that sets out a new time-frame for completion and indicating the basis for the request.

Step 7: If the Board determines to take final action in contravention of GAC advice, then the Board will issue a final decision, stating the reasons why the GAC advice was not followed, as required in Article XI section 2.1.k of the ICANN Bylaws. The Board's final decision and explanation will be posted on ICANN's site.

REFERENCE MATERIALS TO NGPC SUBMISSION 2014.10.12.NG2d

TITLE: RECONSIDERATION REQUEST 14-37

Summary Background

While the full background can be found in the documentation attached to these Reference Materials, Reconsideration Request 14-37 filed by iRegistry Ltd. ("Requester") asks the Board (or here the NGPC) to reverse Resolutions 2014.07.30.NG01 – 2014.07.30.NG04 (the "Resolution") "or at least amend[]" the Resolution, and to then put the decision as to how to address name collisions "on hold" until the issues the Requester raises have "been solved." (Request, § 3, Pg. 3; *id*., § 9, Pg. 18.)

The BGC considered Reconsideration Request 14-37 at its 4 September 2014 meeting and concluded that the Requester has not stated proper grounds for reconsideration. As detailed in the Recommendation and the documents attached to these Reference Materials, the BGC concluded that: (i) there is no evidence that the NGPC's actions in adopting the Resolution support reconsideration; (ii) the Requester has not demonstrated that the NGPC failed to consider any material information in passing the Resolution or that the NGPC relied on false or inaccurate material information in passing the Resolution; and (iii) the Requester has not demonstrated that it has been materially affected by the Resolution. The BGC recommended to the NGPC that Reconsideration Request 14-37 be denied without further consideration.

Document/Background Links

The following attachments are relevant to the BGC's recommendation regarding Reconsideration Request 14-37.

Attachment A is Reconsideration Request 14-37, submitted on 19 August 2014.

Attachment B is Attachments A-H to Request 14-37, submitted on 19 August 2014.

Attachment C is the BGC's Recommendation on Reconsideration Request 14-37, issued on 4 September 2014.

Attachment D is the Clarification to Reconsideration Request 14-37 from I-Registry Ltd., submitted on 11 September 2014.

Attachment E is the SSAC057: SSAC Advisory on Internal Name Certificates, issued on 15 March 2013.

Attachment F is the study prepared by Interisle Consulting Group, entitled Addressing the Consequences of Name Collisions, submitted on 5 August 2013.

Attachment G is the Report of Public Comments from the public comment period regarding Mitigating the Risk of DNS Namespace Collisions, which was open from 26 February 2014 through 21 April 2014.

Attachment H is JAS Global Advisors LLC's final version of its Phase One Report on Mitigating the Risk of DNS Namespace Collisions, submitted on 4 June 2014.

Attachment I is the SSAC066: SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions, issued on 6 June 2014.

Attachment J are NGPC Resolutions 2014.07.30.NG01 – 2014.07.30.NG04, adopting the Name Collision Occurrence Management Framework, approved on 30 July 2014.

Attachment K is the public comment forum regarding Implementing Rights Protection Mechanisms in the Name Collision Mitigation Framework, which will run from 25 August 2014 through 7 October 2014.

Submitted by:	Amy A. Stathos, Deputy General Counsel
Date Noted:	29 September 2014
Email:	amy.stathos@icann.org

Reconsideration Request Form

Version of 11 April 2013

ICANN's Board Governance Committee is responsible for receiving requests for reconsideration from any person or entity that has been materially affected by any ICANN staff action or inaction if such affected person or entity believes the action contradicts established ICANN policies, or by actions or inactions of the Board that such affected person or entity believes has been taken without consideration of material information. Note: This is a brief summary of the relevant Bylaws provisions. For more information about ICANN's reconsideration process, please visit http://www.icann.org/en/general/bylaws.htm#IV and http://www.icann.org/en/committees/board-governance/.

This form is provided to assist a requester in submitting a Reconsideration Request, and identifies all required information needed for a complete Reconsideration Request. This template includes terms and conditions that shall be signed prior to submission of the Reconsideration Request.

Requesters may submit all facts necessary to demonstrate why the action/inaction should be reconsidered. However, argument shall be limited to 25 pages, double-spaced and in 12 point font.

For all fields in this template calling for a narrative discussion, the text field will wrap and will not be limited.

Please submit completed form to reconsideration@icann.org.

1. Requester Information

Name: Anschelika Smoljar

Address: I-REGISTRY Ltd., Contact Information Redacted

Email: Contact Information Redacted

Phone Number (optional):

(Note: ICANN will post the Requester's name on the Reconsideration Request page at http://www.icann.org/en/committees/board-governance/requests-for-reconsideration-en.htm. Requestors address, email and phone number will be removed from the posting.)

2. Request for Reconsideration of (check one only):

_x__ Board action/inaction

___ Staff action/inaction

3. Description of specific action you are seeking to have reconsidered.

(Provide as much detail as available, such as date of Board meeting, reference to Board resolution, etc. You may provide documents. All documentation

provided will be made part of the public record.)

I-REGISTRY is challenging ICANN's inaction in not stopping or at least amending the decision by the NGPC about the Name Collision Occurrence Management Framework Implementation:

- The NGPC made a decision about the Name Collision Occurrence Management Framework Implementation on August 1, 2014.

(see https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en and http://newgtlds.icann.org/sites/default/files/agreements/name-collision-assessment-04aug14-en.pdf)

4. Date of action/inaction:

(Note: If Board action, this is usually the first date that the Board posted its resolution and rationale for the resolution or for inaction, the date the Board considered an item at a meeting.)

The NGPC meeting took place July 30, 2014 with the topic "Name Collision Occurrence Management Framework Implementation" on the agenda (https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en). The decision by the NGPC has been published on August 1, 2014 (https://www.icann.org/news/announcement-2-2014-08-01-en).

5. On what date did you became aware of the action or that action would not be taken?

(Provide the date you learned of the action/that action would not be taken. If more than fifteen days has passed from when the action was taken or not taken to when you learned of the action or inaction, please provide discussion of the gap of time.)

We have been informed by ICANN via E-Mail on August 4, 2014 (see Attachment A) with the document "NAME COLLISION OCCURRENCE ASSESSMENT" published at http://newgtlds.icann.org/sites/default/files/agreements/name-collision-assessment-04aug14-en.pdf

6. Describe how you believe you are materially affected by the action or inaction:

ICANN did not involve the broader ICANN community in the discussion about the Implementation of the Name Collision Occurrence Management Framework despite pretending to do so (as referenced in the rationale for the decision by the NGPC). As involvement is essential for the acceptance and communication of this topic, Registries such as I-REGISTRY will suffer materially from non-

communication and non-acceptance.

ICANN did not try to harmonize the Name Collision Occurrence Management Framework Implementation across all gTLDs, no matter whether in operations or not yet. As a simple, unified process where and how to register domain names is key for registrants, registrar, and registries, I-REGISTRY expects confused registrants and registrar and thus will suffer economically from a non-harmonization.

ICANN did not yet provide registries and registrars with clear rules and guidance. As it is still missing how to allocate names from the name collision list, I-REGISTRY expects that in doubt registrars will not offer domain name registrations from Name Collision lists.

Albeit a path forward has been described in the Name Collision Occurrence Management Framework Implementation, ICANN reserves the right to withhold names even beyond the proposed release date in general.

As a result, both confused registrants and Internet users will lead to lower registration rates of New gTLD domain names and less usage of New gTLD domain names. Both effects will affect Registries materially.

7. Describe how others may be adversely affected by the action or inaction, if you believe that this is a concern.

Registrants are affected

We believe that registrants interested in the new TLDs at-large will be materially affected. There is no central website which lists all TLDs and shows the different categories of TLDs according to the Name Collision Occurrence Management Framework Implementation.

Also, there has been only one press release which for sure did not reach the majority of potential registrants of a domain name globally. A Google search for "Name Collision Occurrence Management Framework Implementation" shows 9 hits (Attachment B).

Trademark holders will be affected by the decision since the existing RPM rules do not consider the allocation and activation of APD names.

Overall, we do believe that the overall majority of registrants is not aware of this issue and this will result in registrants' confusion about the availability of domain names in general.

The technical community and Registrants will be affected

The use and communication of the IP for affected names according to the Name Collision Occurrence Management Framework Implementation is widely unknown to registrars, Internet users and even within the Domain Name Industry.

As of today, we haven't seen any information about the resolution by the NGPC about the Name Collision Occurrence Management Framework Implementation

in publications or member information to tech association, special interest media beyond the press release ICANN sent on August 4, 2014.

The ICANN community is affected

Also, we believe that not taking the views of the ICANN community into account before making a decision contradicts the Bylaws of ICANN. As stated in the Bylaws Article I: MISSION AND CORE VALUES, Section 2. CORE VALUES: “4. Seeking and supporting broad, informed participation reflecting the functional, geographic, and cultural diversity of the Internet at all levels of policy development and decision-making.
(https://www.icann.org/resources/pages/bylaws-2012-02-25-en#III)

Among others, ALAC stated concerns during their exchange with the GAC which has been noted in the GAC Communiqué after the ICANN meeting in Durban:

“…The ALAC voiced concerns regarding issues on dot-less domains and **domain name collisions**…” (Attachment C).

There is no indication that the GAC has been given the opportunity to provide feedback to any of the proposals by JAS Global Advisors LLC and the advice from the Security and Stability Advisory Committee (SSAC) since the ICANN meeting in Durban as there is no publicly available comment issued by the GAC on this topic.

Registries are affected

We believe that not only I-REGISTRY is affected but all Registries which are not yet delegated. Both, confused registrants and Internet users will lead to lower registration rates of New gTLD domain names and less usage of New gTLD domain names. Both effects will affect Registries materially.

8. Detail of Board or Staff Action – Required Information

Staff Action: If your request is in regards to a staff action or inaction, please provide a detailed explanation of the facts as you understand they were provided to staff prior to the action/inaction presented to the staff and the reasons why the staff's action or inaction was inconsistent with established ICANN policy(ies). Please identify the policy(ies) with which the action/inaction was inconsistent. The policies that are eligible to serve as the basis for a Request for Reconsideration are those that are approved by the ICANN Board (after input from the community) that impact the community in some way. When reviewing staff action, the outcomes of prior Requests for Reconsideration challenging the same or substantially similar action/inaction as inconsistent with established ICANN policy(ies) shall be of precedential value.

Board action: If your request is in regards to a Board action or inaction, please provide a detailed explanation of the material information not considered by the Board. If that information was not presented to the Board, provide the reasons why you did not submit the material information to the Board before it acted or

failed to act. “Material information” means facts that are material to the decision.

If your request is in regards to a Board action or inaction that you believe is based upon inaccurate, false, or misleading materials presented to the Board and those materials formed the basis for the Board action or inaction being challenged, provide a detailed explanation as to whether an opportunity existed to correct the material considered by the Board. If there was an opportunity to do so, provide the reasons that you did not provide submit corrections to the Board before it acted or failed to act.

Reconsideration requests are not meant for those who believe that the Board made the wrong decision when considering the information available. There has to be identification of material information that was in existence of the time of the decision and that was not considered by the Board in order to state a reconsideration request. Similarly, new information – information that was not yet in existence at the time of the Board decision – is also not a proper ground for reconsideration. Please keep this guidance in mind when submitting requests.

Provide the Required Detailed Explanation here:

(You may attach additional sheets as necessary.)

We provided a detailed letter to the NGPC well in advance to the meeting (Attachment D), receipt has been confirmed by Mr Chalaby, Chair of the NGPC (Attachment E).

In this letter (Attachment D) we noted that:

1. The proposal does provide uncertainty to registrants into which category a gTLD falls and thus lacks guidance which rights protection mechanisms are available.

2. The proposal has not been agreed-upon by the ICANN community at-large, in contrast to the development of the RPM rules where the community was involved.

We requested that:

1. ICANN, together with the community, extend the existing RPM rules for the allocation and activation of APD names.

2. ICANN takes into account the different registration models and phases of existing and future gTLD operators.

3. ICANN together with the community al-large develops a set of common rules, valid for all gTLDs.

4. Those common rules should apply to both, already delegated gTLDs and not-yet delegated gTLDs, to avoid registrant confusion.

5. Provide Registries with a limited timeframe to either stay with their existing policies or develop new one for the allocation and activation of names of their APD list under the to-be-developed RPM rules.

The NGPC failed to consider Input from stakeholders other than the SSAC and ICANN community at-large. The community at-large were allowed to provide input until April 21, 2014 but not after that date:

> *What Stakeholders or others were consulted?*
>
> *ICANN initiated a public comment forum from **26 February to 21 April** 2014, inviting the community to provide feedback on the JAS Study and Name Collision Framework. During the public comment period, twenty-eight comments were received. The public comment report summarizing the comments, and the full comments can be found at: https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf [PDF, 230 KB].*
>
> *The SSAC also was consulted and offered advice and recommendations to the Board (via SAC066) on the proposed name collision framework included in the JAS Study and Name Collision Framework. Additionally, ICANN **presented** a version of the proposed Final Name Collision Framework during the ICANN Meeting in London.*

The NGPC failed to take material input from the community into account. Also,

the NGPC did not properly assess the implications of the decision.

In their rationale for the decision the NGPC did not mention the letter nor any of the arguments provided by I-Registry and why they have not been considered.

Interestingly, several members of the ICANN community provided their input to the NGPC, too. Apparently the NGPC neither considered them nor provided a rationale why the arguments have not been considered, but did consider only one a few topics as listed in their rationale:

> *Whereas, the NGPC acknowledges comments from the community concerning the **need to ensure that all names**, which registries blocked under their Alternate Path to Delegation Report, **be subject to the rights protection mechanisms** established by the New gTLD Program.*
>
> *(emphasize added)*
>
> *AND:*
>
> ***What concerns or issues were raised by the community?***
>
> *The JAS Study and Name Collision Framework received twenty-eight comments during the public comment period which were submitted by a full range of sources, including New gTLD applicants and those affiliated with applicants, corporations not directly affiliated with applicants,*

individual technology experts, and various DNS related industry organizations. Members of the community also submitted correspondence to ICANN regarding the intersection of name collision issues and rights protection mechanisms. Additionally, the SSAC raised some concerns in SAC066 regarding the name collision framework.

Some key themes and concerns expressed by the SSAC and ICANN community included, but are not limited to the following:

- *Concerns related to the current use of the Second Level Domain (SLD) Block Lists and the Alternate Path to Delegation in general.*

- *Concerns that the proposed 120-day "controlled interruption" period is too long and/or not justified – Some commenters suggested that there is no data to support having a 120-day controlled interruption period, and suggested that if there is a period, it should fall in the range of 45 days to 90 days.*

- *Concerns for using a "loopback" approach instead of a "honeypot" approach – The SSAC recommended that using a honeypot approach allows better notification for HTTP cases, and provides support for IPv4 and IPv6. Some of the public comments also suggest that a honeypot approach would provide a better opportunity to inform users of impending problems. Some other commenters, however, note that a honeypot may expose*

personally identifiable or sensitive information outside of the local network or to potential attackers, among other issues.

- *Concerns about whether the controlled interruption should be continuous or intermittent – The SSAC recommended that instead of a single controlled interruption period, ICANN should introduce rolling interruption periods, broken by periods of normal operation, to allow affected end-user systems to continue to function during the test period with less risk of catastrophic business impact.*
- *Concerns about what type of event would trigger an emergency response – The SSAC recommended that ICANN should expand the range of situations that would trigger an emergency response, for example national security, emergency preparedness, critical infrastructure, key economic processes, commerce, and the preservation of law and order. Some of the public comments also raised concern that a "clear a present danger to human life" standard draws an arbitrary line, and others suggest that certain significant dangers to the business and financial sectors of the global economy might also merit the use of emergency measures.*
- *Concerns about the treatment of .CORP, .HOME, and .MAIL – Some of the public comments support the treatment of .CORP, .HOME, and .MAIL recommending in the JAS Study and Name Collision Framework, while others suggest that a final decision on this matter 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.

- *Comments requesting the acceleration and closure of the collisions issue in general - Some members of the community noted a general concern that the name collision matter is being dealt with at such a late stage of the New gTLD process, and questioned why ICANN did not address the matter sooner. Commenters raising concerns about timing also requested that ICANN take action on the matter with deliberate speed so as not to cause further delay.*

- *Comments expressing concern about the interaction between the name collision block lists and intellectual property rights protection mechanisms – Some public comments and correspondence to ICANN suggest that all names, which registries blocked 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), or other similar mechanism to protect rights holders. Additionally, some .BRAND TLD applicants note many of the "brand" terms included in the block lists are trademarks for the brand's products and services, and are seemingly generated at the root by the brand itself. These commenters suggest that ICANN consider an alternative process for .BRAND TLD applicants to expedite the release of such*

trademarked terms for their immediate use.

(https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en)

To the contrary, the answer from the NGPC to stakeholders which provided their input to the NGPC were standardized letters which have been received by many other members of the ICANN community (Attachment F, Attachment G, Attachment H).

Despite our proposals and the proposal brought forward by the community how to address the open issues, the NGPC filed their decision. This decision includes many open issues which are stated in their “Rationale” and respectively in their “Requirements for ICANN”. In detail the following topics according to the NGPC have to be discussed with affected stakeholders or have to be defined by ICANN staff in the future:

Rationale for Resolution 2014.07.30.NG01 – 2014.07.30.NG04

a) Resolved (2014.07.30.NG01), the NGPC adopts the Name Collision Occurrence Management Framework ….. As part of implementation, **registry operators will be provided with a Name Collision Occurrence**

Assessment (see Registry Agreement, Specification 6, Section 6), which will address, among other things, procedures to remove second level domains from the block list including measures to protect rights holders.…

b) Resolved (2014.07.30.NG02), the NGPC directs the President and CEO, or his designee(s), **to consult with the community during the next 90 days from the publication of these resolutions to address appropriate rights protection mechanisms** for names included in a registry operator's Alternate Path to Delegation Report and recorded in the Trademark Clearinghouse that registry operator withheld from allocation during its Sunrise period or Claims period…

(Emphasize added)

Requirements for ICANN:

c) Work within the IETF and with other relevant technical communities **to identify a notification mechanism for IPv6 that provides similar functionality to that available in IPv4's "Loopback" reserved prefix**…..

d) **Produce new outreach and informational materials** as needed to alert potentially affected parties about name collisions, and link to existing information regarding name collisions developed as part of the initial

outreach campaign.

(Emphasize added)

It seems that the decision has been taken in a hurry to address requests by some stakeholders to move forward.

9. What are you asking ICANN to do now?

(Describe the specific steps you are asking ICANN to take. For example, should the action be reversed, cancelled or modified? If modified, how should it be modified?)

I-REGISTRY seeks immediate reconsideration by the BGC that the decision has to be put on-hold as long as the above mentioned issues have not been solved.

I-REGISTRY requests from the BGC that the decision has to be modified taking input from the ICANN community properly into account.

I-REGISTRY requests from the BGC that the Implementation of the Name Collision Occurrence Management Framework and the release of the concerned names shall be harmonized across all new gTLDs.

10. Please state specifically the grounds under which you have the

standing and the right to assert this Request for Reconsideration, and the grounds or justifications that support your request.

(Include in this discussion how the action or inaction complained of has resulted in material harm and adverse impact. To demonstrate material harm and adverse impact, the requester must be able to demonstrate well-known requirements: there must be a loss or injury suffered (financial or non-financial) that is a directly and causally connected to the Board or staff action or inaction that is the basis of the Request for Reconsideration. The requestor must be able to set out the loss or injury and the direct nature of that harm in specific and particular details. The relief requested from the BGC must be capable of reversing the harm alleged by the requester. Injury or harm caused by third parties as a result of acting in line with the Board's decision is not a sufficient ground for reconsideration. Similarly, injury or harm that is only of a sufficient magnitude because it was exacerbated by the actions of a third party is also not a sufficient ground for reconsideration.)

We believe that this decision has to be put on-hold to enable a proper discussion and implementation guideline within the community. As long as this is not guaranteed I-REGISTRY, all other gTLD applicants and their stakeholders alike suffer from uncertainty how to setup their registration policies, business models, prices and allocation mechanisms. Therefore I-REGISTRY has the standing to ask for Reconsideration.

We believe that this decision has to be put on-hold so that ICANN can start with the announced initial outreach campaign. As long as this campaign has not been executed, neither Registrants, Internet users, IT administrators nor other affected parties will understand what “Name Collision Occurrence” is, how it affects them and thus refrain from registering domain names under new gTLDs. This will materially affect Registries including I-REGISTRY and therefore I-REGISTRY has the standing to ask for reconsideration.

We believe that I-REGISTRY suffers material harm from the decision by the NGPC: Registrants will be confused which names are available for registration on the one hand and Internet users on the other hand about the error provided via the special IP Address (127.0.53.53). This confusion will for sure lead to less registrations and therefore a financial loss of I-REGISTRY. As there is no information provided by a neutral party no Registrant is able to find information online which category a TLD belongs to and thus does not know which domain names are available at which dates.

The requested steps described in #9 including on-hold, discussion among the ICANN community and harmonization across all gTLDs would eliminate the confusion of registrants, which domains can be registered under which circumstances and dates under certain TLDs.

11. Are you bringing this Reconsideration Request on behalf of multiple

persons or entities? (Check one)

____ Yes

__x__ No

11a. If yes, Is the causal connection between the circumstances of the Reconsideration Request and the harm the same for all of the complaining parties? Explain.

Do you have any documents you want to provide to ICANN?

If you do, please attach those documents to the email forwarding this request. Note that all documents provided, including this Request, will be publicly posted at http://www.icann.org/en/committees/board-governance/requests-for-reconsideration-en.htm.

See Attachments A-H.

Terms and Conditions for Submission of Reconsideration Requests

The Board Governance Committee has the ability to consolidate the

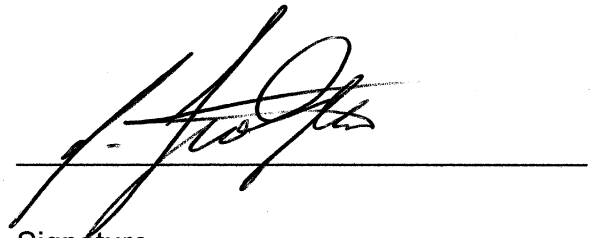
consideration of Reconsideration Requests if the issues stated within are sufficiently similar.

The Board Governance Committee may dismiss Reconsideration Requests that are querulous or vexatious.

Hearings are not required in the Reconsideration Process, however Requestors may request a hearing. The BGC retains the absolute discretion to determine whether a hearing is appropriate, and to call people before it for a hearing.

The BGC may take a decision on reconsideration of requests relating to staff action/inaction without reference to the full ICANN Board. Whether recommendations will issue to the ICANN Board is within the discretion of the BGC.

The ICANN Board of Director's decision on the BGC's reconsideration recommendation is final and not subject to a reconsideration request.



August 13, 2014

Signature Date

(Anschelika Smoljar, Executive Director)

Attachment A

Von: Contact Information Redacted

Gesendet: Montag, 4. August 2014 23:37
An: Contact Information Redacted
Betreff: Auction Schedule and the Name Collision Occurrence Management Framework

New Generic Top-Level Domains

As you may have seen, ICANN announced the finalized Name Collision Occurrence Management Framework ("the Framework") (https://www.icann.org/news/announcement-2-2014-08-01-en). To learn more about name collisions, including the Framework, please see: www.ICANN.org/namecollision.

Applicants who received an intent to Auction notification were provided an opportunity to request an Auction postponement pending finalization of the Framework. These postponements were accommodated on a per Auction basis. Because the Framework has now been finalized, postponement requests on the basis of pending finalization of the Framework will no longer be accommodated after the August Auction.

The current Auction Schedule can be found at http://newgtlds.icann.org/en/applicants/auctions, additionally you can view the planned Auction Date for an unresolved contention set on the Contention Set Status page. Applicants will receive a confirmation of the Auction Date at least 21 days in advance of the Auction. Applicants may request to advance or postpone an Auction Date, provided the request is made by each and every member of the contention set, please refer to the Auction Date Advancement/Postponement Request Form for more details.

Any Questions?

Please provide any questions by logging into the customer service portal and submitting a case, or sending an email to: Contact Information Redacted

Disclosure
This notification is not application specific and will only be received once per unique Primary Contact email address.

Best Regards,

Attachment B

"Name Collision Occurrence Management Framework Implementation"

Anmelden

Web Bilder News Videos Shopping Mehr Suchoptionen

9 Ergebnisse (0,27 Sekunden)

ICANN Approves Name Collision Occurrence Management ...
https://www.icann.org/.../announcement-2-2014-08-... Diese Seite übersetzen
01.08.2014 - Overview: **Name Collision Occurrence Management Framework Implementation**. ICANN registry operators are obligated to comply with ...

name collision occurrence management framework ...
redhotgeek.com/index.php?...**name_collision_occur**... Diese Seite übersetzen
name collision occurrence management framework implementation Name Collision Occurrence Management Framework ICANN and the multistakeholder ...

Middle East Network Operators Group List () - Gmane
comments.gmane.org/gmane.org.operators.../663 Diese Seite übersetzen
04.08.2014 - Overview: **Name Collision Occurrence Management Framework Implementation**. ICANN registry operators are obligated to comply with ...

Africa Registry News
www.africaregistry.com/about_africa/news.htm Diese Seite übersetzen
05.08.2014 - For more information see the **Name Collision Occurrence Management Framework Implementation** Announcement [...] ICANN Approves ...

ICANN will be holding a webinar to provide information ...
news.domfinder.com/.../30661742-icann-join-us-fo... Diese Seite übersetzen
For more information see the **Name Collision Occurrence Management Framework Implementation** Announcement [PDF, 634 KB]. Webinar Details Session 1 ...

mrarrowhead.com - php tutorials, web design - Facebook
www.facebook.com/permalink.php?id...story... Diese Seite übersetzen
name collision occurrence management framework implementation. ICANN and the multi-stakeholder community has announced the implementation of The ...

News & Articles Archives - Page 4 of 5668 - iGoldRush ...
www.igoldrush.com/news/2014/08/page/4 Diese Seite übersetzen
02.08.2014 - For more information see the **Name Collision Occurrence Management Framework Implementation** [...] Continue reading → · DomainPulse.com ...

DomainPulse.com - The Beat on the Domain Name Industry ...
feedage.com:8080/.../domainpulsecom-the-beat-on-... Diese Seite übersetzen
... operator requirements followed by a Q&A. For more information see the **Name Collision Occurrence Management Framework Implementation** Announcement ...

Domain News Headlines - DNHeadlines.com
dnheadlines.com/domain-news-by-date.php
... operator requirements followed by a Q&A. For more information see the **Name Collision Occurrence Management Framework Implementation** Announcement ...

Damit Sie nur die relevantesten Ergebnisse erhalten, wurden einige Einträge ausgelassen, die den 9 angezeigten Treffern sehr ähnlich sind. Sie können bei Bedarf die Suche unter Einbeziehung der übersprungenen Ergebnisse wiederholen.

Unbekannt - Genauen Standort verwenden - Weitere Informationen

Hilfe Feedback geben Datenschutzerklärung & Nutzungsbedingungen

Attachment C

Governmental Advisory Committee

Durban, 18 July 2013

GAC Communiqué – Durban, South Africa[1]

I. Introduction

The Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) met in Durban, South Africa during the week of 13 July 2013. 59 GAC Members and 4 Observers attended the meetings. The GAC expresses warm thanks to the local host, .zadna, for their support.

II. Inter-constituency Activities

1. Briefing from the Geo TLD Registry Group

The GAC met with the Geo TLD Registry Group and received information on the organization's origins, values, missions and current concerns.

2. Meeting with the Accountability and Transparency Review Team 2 (ATRT 2)

The GAC met with the ATRT 2 and discussed expectations and priorities. The GAC encouraged the ATRT2 to give advice on improving the accountability and transparency in ICANN's financial operations reporting. The ATRT2 was invited to advise on how to improve outreach and active participation, especially from developing countries. Broad participation of stakeholders from all regions is vital for the legitimacy of ICANN and the multi-stakeholder model. The GAC also invited the ATRT2 to give advice on how to improve the GAC and the transparency of GAC meetings, and to better explain and provide rationales for the advice of the GAC. The ATRT2 invited individual GAC members to provide further written inputs to the Review Team.

[1] To access previous GAC advice, whether on the same or other topics, past GAC communiqués are available at: https://gacweb.icann.org/display/gacweb/GAC+Recent+Meetings and older GAC communiqués are available at: https://gacweb.icann.org/display/gacweb/GAC+Meetings+Archive.

3. **Meeting with the Generic Names Supporting Organization (GNSO)**

   The GAC met with the GNSO and exchanged views on key policy development work in the GNSO, including an ongoing Policy Development Process (PDP) regarding protection of IGO and INGO names and acronyms. An exchange focused on the opportunities for the GAC to engage early in GNSO Policy Development Processes.

4. **Meeting with the Security and Stability Advisory Committee (SSAC)**

   The GAC met with the SSAC and received an update on recent SSAC work regarding namespace collisions, internal name certificates and dotless domains, and exchanged views on ensuing concerns.

5. **Meeting with the Country Code Names Supporting Organization (ccNSO)**

   The GAC met with the ccNSO and received information about the recently concluded policy development regarding IDN ccTLDs, the modification of the IDN Fast Track process with creation of a second panel and the Framework of Interpretation work. The GAC and the ccNSO also discussed how to further improve the future dialogue between the GAC and the ccNSO.

6. **Meeting with the At-Large Advisory Committee (ALAC)**

   The GAC met with the ALAC and received an introduction to ALAC's organization, bottom-up processes and output, including formal ALAC objections to certain new gTLD applications. The ALAC voiced concerns regarding issues on dot-less domains and domain name collisions and expressed support for recent SSAC statements. The ALAC also expressed concerns over the high threshold in the dispute resolution procedure for Public Interest Commitments (PIC) in particular in relation to the measurable harm standard required to file a complaint and the enforcement of these.

7. **Briefing from the Domain Name Association (DNA)**

   The GAC met with the Domain Name Association and received information on its structure and objectives.

8. **Meeting with the Expert Working Group on gTLD Directory Services (EWG)**

   The GAC met with the EWG and exchanged views on the model proposed by the EWG for the next generation directory service as a successor to the WHOIS service.

The GAC referenced its WHOIS principles from 2007 and its Beijing advice regarding the WHOIS Review Team recommendations, which both have served as input for the work of the EWG. The GAC expressed its concerns about the risks associated with centralized storage of data in one repository in one jurisdiction, and raised a series of issues relating to the proposed data repository structure and access including security, data accuracy, consistency with national law, accreditation of database users, and privacy governance. The GAC looks forward to further discussion of these issues as the working group progresses.

9. Briefing from Architelos

The GAC received a briefing on the TLD market and its development from Architelos, a consultancy focused on the domain name industry.

***

The GAC warmly thanks the GNSO, the SSAC, the ccNSO and the ALAC, as well as all those among the ICANN community who have contributed to the dialogue with the GAC in Durban.

III. Internal Matters

1. The GAC held its second capacity building session for new and existing members on 13 July, which included an update to the GAC on internationalization and the ICANN's strategy for engagement in the Africa region.
2. The GAC welcomed Madagascar, Namibia, São Tomé and Príncipe, Swaziland, and Zambia to the GAC as members.
3. The chair and vice chairs provided an update in Durban on progress with regard to ACIG providing secretariat support to the GAC.

IV. GAC Advice to the Board[2]

1. New gTLDs

1. GAC Objections to Specific Applications (ref. Beijing Communiqué 1.c.)

a. The GAC Advises the ICANN Board that:

i. The GAC has reached consensus on GAC Objection Advice according to Module 3.1 part I of the Applicant Guidebook on the following applications:[3]

[2] To track the history and progress of GAC Advice to the Board, please visit the GAC Advice Online Register available at: https://gacweb.icann.org/display/GACADV/GAC+Register+of+Advice

[3] Module 3.1: "The GAC advises ICANN that it is the consensus of the GAC that a particular application should not proceed. This will create a strong presumption for the ICANN Board that the application should not be approved.

1. The application for .amazon (application number 1-1315-58086) and related IDNs in Japanese (application number 1-1318-83995) and Chinese (application number 1-1318-5591)
2. The application for .thai (application number 1-2112-4478)

b. guangzhou (IDN in Chinese), shenzhen (IDN in Chinese), .spa and .yun

i. The GAC agrees to leave the applications below for further consideration and **advises the ICANN Board**:

i. Not to proceed beyond initial evaluation until the agreements between the relevant parties are reached.

1. The applications for .spa (application number 1-1309-12524 and 1-1619-92115)
2. The application for .yun (application number 1-1318-12524
3. The application for .guangzhou (IDN in Chinese - application number 1-1121-22691)
4. The application for .shenzhen (IDN in Chinese - application number 1-1121-82863)

2. .wine and .vin (ref. Beijing Communiqué 1.c.)

a. **The GAC advises the ICANN Board that:**

i. The GAC considered the two strings .vin and .wine and due to the complexity of the matter was unable to conclude at this meeting. As a result the GAC agreed to take thirty days additional time with a view to conclude on the matter.

3. .date and .persiangulf (ref. Beijing Communiqué 1.c.)

a. **The GAC has finalised its consideration of the following strings, and does not object to them proceeding:**

i. .date (application number 1-1247-30301)

ii. .persiangulf (application number 1-2128-55439)

4. .indians and .ram

a. The GAC Advises the ICANN Board that:

i. The GAC has noted the concerns expressed by the Government of India not to proceed with the applications for .indians and .ram.

5. Protection of IGO Acronyms

a. The GAC reaffirms its previous advice from the Toronto and Beijing Meetings that IGOs are in an objectively different category to other rights holders thus warranting special protection by ICANN. IGOs perform important global public missions with public funds and as such, their identifiers (both their names and their acronyms) need preventative protection in an expanded DNS.

b. The GAC understands that the ICANN Board, further to its previous assurances, is prepared to fully implement GAC advice; an outstanding matter to be finalized is the practical and effective implementation of the permanent preventative protection of IGO acronyms at the second level.

c. The GAC advises the ICANN Board that:

i. The GAC is interested to work with the IGOs and the NGPC on a complementary cost-neutral mechanism that would:

a. provide notification to an IGO if a potential registrant seeks to register a domain name matching the acronym of an IGO at the second level, giving the IGO a reasonable opportunity to express concerns, if any; and

b. allow for an independent third party to review any such registration request, in the event of a disagreement between an IGO and potential registrant.

ii. The initial protections for IGO acronyms confirmed by the NGPC at its meeting of 2 July 2013 should remain in place until the dialogue between the GAC, NGPC, and IGO representatives ensuring the implementation of preventative protection for IGO acronyms at the second level is completed.

5. Protection of Red Cross/Red Crescent Acronyms

a. The GAC advises the ICANN Board that

i. The same complementary cost neutral mechanisms to be worked out (as above in 4.c.i.) for the protection of acronyms of IGOs be used to also protect the acronyms of the International Committee

of the Red Cross (ICRC/CICR) and the International Federation of Red Cross and Red Crescent Societies (IFRC/FICR).

6. Category 1 Safeguard Advice

i. The GAC has met with the NGPC to discuss the Committee's response to GAC advice contained in the Beijing Communique on safeguards that should apply to Category 1 new gTLDs. **The GAC Advises the ICANN Board that:**

1. The GAC will continue the dialogue with the NGPC on this issue.

7. Geographic Names and Community Applications

a. Geographic Names

i. The GAC recommends that ICANN collaborate with the GAC in refining, for future rounds, the Applicant Guidebook with regard to the protection of terms with national, cultural, geographic and religious significance, in accordance with the 2007 GAC Principles on New gTLDs.

b. Community Applications

i. The GAC reiterates its advice from the Beijing Communiqué regarding preferential treatment for all applications which have demonstrable community support, while noting community concerns over the high costs for pursuing a Community Objection process as well as over the high threshold for passing Community Priority Evaluation.

ii. Therefore the GAC advises the ICANN Board to:

a. Consider to take better account of community views, and improve outcomes for communities, within the existing framework, independent of whether those communities have utilized ICANN's formal community processes to date.

8. DNS Security and Stability

a. The GAC shares the security and stability concerns expressed by the SSAC regarding Internal Name Certificates and Dotless Domains. The GAC requests the ICANN Board to provide a written briefing about:

i. how ICANN considers this SSAC advice with a view to implementation as soon as possible. The GAC believes that all such stability and security analysis should be made publicly available prior to the delegation of new gTLDS.

ii. **The GAC Advises the ICANN Board to:**

a. As a matter of urgency consider the recommendations contained in the SSAC Report on Dotless Domains (SAC053) and Internal Name Certificates (SAC057).

9. Registry and Registrar Agreements and Conflicts with Law

a. It was noted that there are provisions in the Registry Agreement and Registrar Accreditation Agreement that may conflict with applicable law in certain countries, in particular privacy and data retention, collection and processing law. The importance of having adequate procedures to avoid these conflicts was highlighted.

V. Next Meeting

The GAC will meet during the 48th ICANN meeting in Buenos Aires, Argentina.

Attachment D

I-REGISTRY®
YOUR PROFESSIONAL DOMAIN SOLUTION

I-REGISTRY LTD.
Contact Information Redacted

Contact Information Redacted

Cherine Chalaby
Chair, New gTLD Program Committee
Internet Corporation for Assigned Names and Numbers
Contact Information Redacted

via email to Contact Information Redacted

July 27, 2014

Re: letter of RySG, IPC and BC on Rights Protection Mechanism to Name Collision Blocklists

Dear Mr Chalaby, dear members of the NGPC,

First of all, we would like to express our support for the letter sent July 17, 2014 on behalf of the RySG, BC and IPC. Although there has been no formal vote on this proposal, we appreciate the initiative taken and outcome.

However, we would like to note that while this proposal serves the needs of both rights owners and registries, we are concerned that registrants might get confused. As we've experienced ourselves, registrants are crucial for the success of the gTLD program and their needs to be taken serious. Many of them do not understand the reasons for reservation and block lists and under which TLDs they can register, allocate or not register names from these lists. Having said this, the goal should be to simplify and unify the release for name collision names across all gTLDs. Therefore, some implications of this proposal need a more thorough analysis:

- The proposal does provide uncertainty to registrants into which category a gTLD falls and thus lacks guidance which rights protection mechanisms are available.
- The proposal has not been agreed-upon by the ICANN community at-large, in contrast to the development of the RPM rules where the community was involved.

Therefore we ask ICANN to thoroughly evaluate the proposed model and we propose that:

- ICANN, together with the community, extend the existing RPM rules for the allocation and activation of APD names.
- ICANN takes into account the different registration models and phases of existing and future gTLD operators.
- ICANN together with the community al-large develops a set of common rules, valid for all gTLDs.
- Those common rules should apply to both, already delegated gTLDs and not-yet delegated gTLDs, to avoid registrant confusion.
- Provide Registries with a limited timeframe to either stay with their existing policies or develop new one for the allocation and activation of names of their APD list under the to-be-developed RPM rules.

We kindly ask the NGPC to take these issues into consideration.

With best regards,

I-REGISTRY Ltd.

- sgd. Anschelika Smoljar -

Attachment E

Von:	Cherine Chalaby Contact Information Redacted
Gesendet:	Dienstag, 29. Juli 2014 09:52
An:	Anschelika Smoljar
Cc:	Akram Atallah; Christine Willett; Megan Bishop; Michelle Bright; Karine Perset
Betreff:	Re: letter of RySG, IPC and BC on Rights Protection Mechanism to Name Collision Blocklists

Dear Anschelika Smoljar,

On behalf of the New gTLD Program Committee (NGPC), I acknowledge receipt of the I-REGISTRY Ltd letter dated July 27, 2014.
Best regards,

Cherine Chalaby
Chair, New gTLD Program Committee

From: Anschelika Smoljar Contact Information Redacted
Date: Monday, 28 July 2014 21:26
To: Cherine Mohsen Chalaby Contact Information Redacted
Cc: Anschelika Smoljar Contact Information Redacted
Subject: Re: letter of RySG, IPC and BC on Rights Protection Mechanism to Name Collision Blocklists

Dear Mr Chalaby,

attached I'm sending you our letter dated July 27 in regard to Rights Protection Mechanism to Name Collision Blocklists

I would appreciate it if you could send me a confirmation of receipt.

Thank you.

Best regards

Anschelika Smoljar

I-REGISTRY Ltd.
Contact Information Redacted

Contact Information Redacted

Contact Information Redacted

Attachment F

The Internet Corporation for Assigned Names and Numbers

8 August 2014

Anschelika Smoljar
I-REGISTRY Ltd.

Re: Letter of RySG, IPC and BC on Rights Protection Mechanism to Name Collision Blocklists

Dear Ms. Anschelika Smoljar:

Thank you for your letter of 27 July 2014. We appreciate I-REGISTRY Ltd's comments, and we have posted the letter to the New gTLD correspondence page (https://www.icann.org/en/system/files/correspondence/smoljar-to-chalaby-27jul14-en.pdf).

As you may be aware, on 30 July 2014, the ICANN Board New gTLD Program Committee (NGPC) approved the Name Collision Occurrence Management Framework (https://www.icann.org/news/announcement-2-2014-08-01-en). The framework implementation requirements were developed with input from many sources including the ICANN community, a report published by JAS Global Advisors LLC, and advice from the Security and Stability Advisory Committee (SSAC). To view the framework, see (https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf).

For information on how the Name Collision Occurrence Management Framework impacts registry operators and new gTLD applicants, we encourage you to participate in the upcoming webinars scheduled for 12 August 2014 (https://www.icann.org/news/announcement-3-2014-08-01-en). Questions for ICANN staff may be submitted in advance to newgtld@icann.org or gdd-communications@icann.org.

We look forward to I-REGISTRY Ltd's continued participation in the multi-stakeholder process.

Sincerely,

Cyrus Namazi
Vice President, Domain Name Services & Industry Engagement
Global Domains Division
ICANN

Los Angeles Contact Information Redacted
Offices: Beijing • Brussels • Istanbul • Montevideo • Singapore • Washington

Attachment G

The Internet Corporation for Assigned Names and Numbers

8 August 2014

Mr. Andrew Merriam
Secretary
The New TLD Applicant Group (NTAG)

Dear Mr. Andrew Merriam and Members of the NTAG:

Thank you for your letter of 25 June 2014. We appreciate the New TLD Applicant Group's (NTAG) comments, and we have posted the letter to the New gTLD correspondence page (http://newgtlds.icann.org/en/program-status/correspondence/ntag-to-atallah-25jun14-en.pdf)

As you may be aware, on 30 July 2014, the ICANN Board New gTLD Program Committee (NGPC) approved the Name Collision Occurrence Management Framework (https://www.icann.org/news/announcement-2-2014-08-01-en). The framework implementation requirements were developed with input from many sources including the ICANN community, a report published by JAS Global Advisors LLC, and advice from the Security and Stability Advisory Committee (SSAC). To view the framework, see (https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf).

For information on how the Name Collision Occurrence Management Framework impacts registry operators and new gTLD applicants, we encourage you to participate in the upcoming webinars scheduled for 12 August 2014 (https://www.icann.org/news/announcement-3-2014-08-01-en). Questions for ICANN staff may be submitted in advance to newgtld@icann.org or gdd-communications@icann.org.

We look forward to the NTAG's continued participation in the multi-stakeholder process.

Sincerely,

Cyrus Namazi
Vice President, Domain Name Services & Industry Engagement
Global Domains Division
ICANN

Los Angeles Contact Information Redacted
Offices: Beijing • Brussels • Istanbul • Montevideo • Singapore • Washington

http://icann.org

Attachment H

The Internet Corporation for Assigned Names and Numbers

8 August 2014

Elisa Cooper
Chair, Business Constituency

Keith Drazek
Chair, Registry Stakeholder Group

Kristina Rosette
President, Intellectual Property Constituency

Re: Application of Rights Protection Mechanism to Name Collision Blocklists

Dear Ms. Cooper, Ms. Rosette, and Mr. Drazek:

Thank you for your letter of 17 July 2014. We appreciate the Registry Stakeholder Group (RySG), the Business Constituency (BC) and the Intellectual Property Constituency's (IPC) comments, and we have posted the letter to the New gTLD correspondence page (https://www.icann.org/en/system/files/correspondence/cooper-et-al-to-chalaby-ngpc-17jul14-en.pdf).

As you may be aware, on 30 July 2014, the ICANN Board New gTLD Program Committee (NGPC) approved the Name Collision Occurrence Management Framework (https://www.icann.org/news/announcement-2-2014-08-01-en). The framework implementation requirements were developed with input from many sources including the ICANN community, a report published by JAS Global Advisors LLC, and advice from the Security and Stability Advisory Committee (SSAC). To view the framework, see (https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf).

For information on how the Name Collision Occurrence Management Framework impacts registry operators and new gTLD applicants, we encourage you to participate in the upcoming webinars scheduled for 12 August 2014 (https://www.icann.org/news/announcement-3-2014-08-01-en). Questions for ICANN staff may be submitted in advance to newgtld@icann.org or gdd-communications@icann.org.

We look forward to the RySG, the BC, and the IPC's continued participation in the multi-stakeholder process.

Sincerely,

Cyrus Namazi
Vice President, Domain Name Services & Industry Engagement
Global Domains Division
ICANN

Contact Information Redacted

RECOMMENDATION

OF THE BOARD GOVERNANCE COMMITTEE (BGC)

RECONSIDERATION REQUEST 14-37

4 SEPTEMBER 2014

Anschelika Smoljar, on behalf of iRegistry Ltd. (the "Requester"), seeks reconsideration of the NGPC's[1] 30 July 2014 Resolution adopting the Name Collision Occurrence Management Framework.

I. Brief Summary.

The Requester is iRegistry, a domain name registry.

On 30 July 2014, the NGPC approved Resolutions 2014.07.30.NG01 – 2014.07.30.NG04 (the "Resolution"), which adopted the Name Collision Occurrence Management Framework (the "Framework"). The Framework sets forth procedures that registries must follow to prevent name collisions[2] from compromising the security or stability of the Internet. The Resolution "directs the [ICANN] President and CEO, or his designee(s), to take the necessary actions to implement" the Framework.[3]

On 13 August 2014, the Requester filed the instant Request seeking reconsideration of the NGPC's Resolution. The Requester argues that the NGPC failed to sufficiently involve the public in its decision to adopt the Framework. The Requester contends that the Framework will

---

[1] New gTLD Program Committee.

[2] A name collision occurs when an attempt to resolve a name used in a private name space (e.g. under a non-delegated Top-Level Domain, or a short, unqualified name) results in a query to the public Domain Name System ("DNS"). *See* https://www.icann.org/resources/pages/name-collision-2013-12-06-en. When the administrative boundaries of private and public namespaces overlap, these name collisions may yield unintended or harmful results.

[3] *See* Resolution, *available at* https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en.

lead to confusion amongst registrants, leading to a lower volume of registrations, and thus adversely impact the Requester financially.

The BGC[4] concludes there is no evidence that the NGPC's actions in adopting the Resolution support reconsideration. As discussed in further detail below, the Requester has not demonstrated that the NGPC failed to consider any material information or relied on false or inaccurate material information in passing the Resolution. As such, the Requester has not stated a proper basis for reconsideration.

II. Facts.

A. Background Facts.

1. Brief Background Regarding Name Collisions.

A name collision occurs when an attempt to resolve a name used in a private name space (e.g., under a non-delegated Top-Level Domain, or a short, unqualified name) results in a query to the public DNS.[5] When the administrative boundaries of private and public namespaces overlap, name resolution may yield unintended or harmful results.[6] The introduction of any new domain name into the DNS creates the potential for name collision. However, name collision has been discussed specifically in the context of the New gTLD Program, because the expansion of new gTLDs has brought renewed attention to the possibility that certain applied-for new gTLDs could be identical to name labels used in private networks.

Accordingly, in furtherance of ICANN's core values aimed at "[p]reserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet"

[4] Board Governance Committee.
[5] *See* https://www.icann.org/resources/pages/name-collision-2013-12-06-en.
[6] For an analogy, consider calling for "Mary" in your office where there's only one "Mary", and then calling out "Mary" in a shopping mall and expecting that "office Mary" will respond. *See* FAQs, *available at*, https://www.icann.org/resources/pages/name-collision-ro-faqs-2014-08-01-en.

(Bylaws, Art. 1, § 2.1), on 15 March 2013, ICANN's Security and Stability Advisory Committee ("SSAC") published SAC057: SSAC Advisory on Internal Name Certificates.[7] The report identified a Certificate Authority ("CA") practice that, if widely exploited, could pose risks to the privacy and integrity of secure Internet communications. The SSAC advised ICANN to take immediate steps to mitigate the risks. The issues identified in SAC 057 are part of the more general category of name collision issues.

On 18 May 2013, the ICANN Board approved a resolution commissioning a study in response to the SSAC's advice in SAC057.[8]

On 5 August 2013, ICANN released the study, prepared by Interisle Consulting Group, of the likelihood and potential consequences of collision between new public gTLD labels and existing private uses of the same strings.[9]

On 7 October 2013, ICANN introduced the New gTLD Collision Occurrence Management Plan ("Plan"), which permitted the use of an alternate path to delegation.[10] As part of the Resolution adopting the Plan, the NGPC recommended "to the ICANN Board that it direct the ICANN President and CEO to develop a long term plan to manage name collision risks related to the delegation of new TLDs, and to work with the community to develop a long-term plan to retain and measure root-server data."[11]

---

[7] *See* https://www.icann.org/en/system/files/files/sac-057-en.pdf.
[8] *See* https://features.icann.org/ssac-advisory-internal-name-certificates.
[9] *See* Addressing the Consequences of Name Collisions, *available at* https://www.icann.org/news/announcement-3-2013-08-05-en.
[10] *See* New gTLD Collision Occurrence Management Plan Frequently Asked Questions, *available at* https://www.icann.org/news/announcement-2013-12-03-en.
[11] *See* https://www.icann.org/resources/board-material/resolutions-new-gtld-2013-10-07-en#1.a.

In November 2013, ICANN engaged JAS Global Advisors LLC ("JAS") to lead the development of the Framework, in cooperation with the community.[12]

From 26 February 2014 through 21 April 2014, ICANN implemented a public comment period where the community provided feedback on possible solutions to the name collision issue, including the issue of implementing a framework to manage and mitigate name collisions; ICANN received 28 comments, none of which were from the Requester.[13]

On 4 June 2014, after collection of community feedback, JAS released the final version of its Phase One Report on Mitigating the Risk of DNS Namespace Collisions.[14]

On 6 June 2014, SSAC published SAC066: SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions, in which it offered advice and recommendations to the Board on the framework presented in the JAS Study and Name Collision Framework.[15]

On 30 July 2014, the NGPC approved Resolutions 2014.07.30.NG01 – 2014.07.30.NG04 ("Resolution"), which adopted the Framework. The Framework sets forth procedures that registries must follow to prevent name collisions from compromising the security or stability of the Internet. The Resolution "directs the [ICANN] President and CEO, or his designee(s), to take the necessary actions to implement" the Framework.[16]

On 4 August 2014, ICANN's Global Domains Division issued each new gTLD registry operator a Name Collision Occurrence Assessment ("Assessment"), which identified which

---

[12] *See* https://www.icann.org/resources/pages/name-collision-2013-12-06-en.
[13] *See* Report of Public Comments, *available at* https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf.
[14] See JAS Report, *available at* https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf.
[15] *See* https://www.icann.org/en/system/files/files/sac-066-en.pdf.
[16] *See* Resolution, *available at* https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en.

measures registries must take to avoid name collision issues, in accordance with the Framework.[17]

On 12 August 2014, ICANN presented a webinar providing an overview of the Framework specifically geared towards registry operators.[18]

While how to treat one category of names affected by the name collision issue is not yet part of the Framework, ICANN is in the process of gathering public input on this topic. Specifically, ICANN has opened a public comment forum on this particular issue, which will run from 25 August 2014 through 7 October 2014.[19]

2. Background Regarding The Request.

The Requester did not participate in the public comment forum ICANN implemented from 26 February 2014 through 21 April 2014, where the community provided feedback on possible solutions to the name collision issue.[20]

On 27 July 2014, the Requester sent a letter to ICANN asking ICANN to "thoroughly evaluate" a proposal for addressing the problem of name collisions and providing five specific proposals as to the how the issue should be addressed. (Request, Ex. D.)

On 29 July 2014, ICANN acknowledged receipt of the Requester's letter. (Request, Ex. E.)

On 30 July 2014, the NGPC approved the Resolution adopting the Framework.[21]

---

[17] *See* Name Collision Occurrence Assessment, *available at* http://newgtlds.icann.org/sites/default/files/agreements/name-collision-assessment-04aug14-en.pdf.
[18] *See* https://www.icann.org/resources/pages/name-collision-2013-12-06-en.
[19] *See* Implementing Rights Protection Mechanisms in the Name Collision Mitigation Framework, *available at* https://www.icann.org/public-comments/name-collision-rpm-2014-08-25-en.
[20] *See* Report of Public Comments, *available at* https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf.
[21] *See* Resolution, *available at* https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en.

On 4 August 2014, the Requester received the Assessment via email. (Request, Ex. A.)

On 13 August 2014, the Requester filed the instant Request, seeking reconsideration of the NGPC's Resolution.

B. The Requester's Claims.

The Requester contends that reconsideration is warranted because the NGPC, in approving the Resolution:

1. "Failed to take material input from the community into account." (Request, § 8, Pg. 11); and
2. "[D]id not properly assess the implications of the [Resolution]." (*Id*., § 8, Pg. 12.).

C. Relief Requested.

The Requester asks the Board to reverse the Resolution "or at least amend[]" it, and to then put the decision as to how to address name collisions "on hold" until the issues the Requester raises have "been solved." (Request, § 3, Pg. 3; *id*., § 9, Pg. 18.) Specifically, the Requester asks that the implementation of the Framework "be harmonized across all gTLDs." (*Id*., § 9, Pg. 18.)

III. Issues.

In view of the claims set forth in Request 14-37, the issues posed by the Requester are whether the NGPC:

1. Failed to consider material input from the community in approving the Resolution (Request, § 8, Pg. 11); and
2. Improperly underestimated the Resolution's potential negative consequences. (*Id*., § 8, Pgs. 7-8.)

IV. The Relevant Standards for Evaluating Reconsideration Requests.

ICANN's Bylaws provide for reconsideration of a Board or staff action or inaction in

accordance with specified criteria.[22] (Bylaws, Art. IV, § 2.) Requester is challenging a Board action. A Board action may be subject to reconsideration where it was undertaken "without consideration of material information, except where the party submitting the request could have submitted, but did not submit, the information for the Board's consideration at the time of action or refusal to act," or, where it was "taken as a result of the Board's reliance on false or inaccurate material information." (Bylaws, Art. IV, § 2.)

Denial of a request for reconsideration of Board action or inaction is appropriate if the BGC recommends, and in this case the NGPC agrees, that the requesting party has not satisfied the reconsideration criteria set forth in the Bylaws. Further, summary dismissal of a request for reconsideration is appropriate if the BGC recommends, and in this case the NGPC agrees, that the requesting party does not have standing because the party "had notice and opportunity to, but did not, participate in the public comment period relating to the contested action, if applicable." (Bylaws, Art. IV, § 2.9.)

V. Analysis and Rationale.

The Requester has not demonstrated that the Board failed to consider material information or relied on false or inaccurate material information in passing the Resolutions; therefore, reconsideration is not appropriate.

[22] Article IV, § 2.2 of ICANN's Bylaws states in relevant part that any entity may submit a request for reconsideration or review of an ICANN action or inaction to the extent that it has been adversely affected by:

> (a) one or more staff actions or inactions that contradict established ICANN policy(ies); or
> (b) one or more actions or inactions of the ICANN Board that have been taken or refused to be taken without consideration of material information, except where the party submitting the request could have submitted, but did not submit, the information for the Board's consideration at the time of action or refusal to act; or
> (c) one or more actions or inactions of the ICANN Board that are taken as a result of the Board's reliance on false or inaccurate material information.

A. The Request Warrants Summary Dismissal.

Section 2.9 of Article IV of ICANN's Bylaws permits the BGC to summarily dismiss a request for reconsideration if "the requestor had notice and opportunity to, but did not, participate in the public comment period relating to the contested action[.]" (Bylaws, Art. IV, § 2.9.) From 26 February 2014 through 21 April 2014, ICANN implemented a public comment period where the community provided feedback on the possible solutions, including a framework, to name collision issues.[23] The public comment forum was announced on ICANN's website so as to provide notice to the community of its existence.[24] The forum generated 28 comments from a wide variety of stakeholders and community members.[25] The comments were used by JAS Global Advisors to modify the proposed framework, "provide a final report," and also "for ICANN to provide a proposal based on input from the community" for the NGPC's consideration.[26] Many concepts and procedures that the Requester discusses in the Request are discussed in the public comments, including the need for outreach and trainings related to any name collision proposals, block list timing, and controlled interruptions.[27]

The Requester did not participate in the public comment forum, and has offered no justification, excuse or explanation for its decision to refrain from doing so. The only communication it claims to have had with ICANN regarding name collisions is a letter dated 27 July 2014, which was well after the public comment period had closed and mere days before the

[23] *See* Report of Public Comments, *available at* https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf.
[24] *See* Public Comment Invited: Implementing Rights Protection Mechanisms in the Name Collision Mitigation Framework, *available at* https://www.icann.org/news/announcement-5-2014-08-25-en.
[25] *Id*.
[26] *Id*.
[27] *Id*.

NGPC approved the Resolution adopting the Framework.[28] Pursuant to Section 2.9 of Article IV of ICANN's Bylaws, and given that the public comment period here indisputably related to the Resolution, summary dismissal is warranted on the basis of the Requester's non-participation. However, in the interest of completeness, the BGC will nonetheless address the merits of the Request.

B. The NGPC Considered All Material Information.

The Requester's suggestion that the NGPC failed to consider material information is not accurate. In order to state a basis for reconsideration of a Board action, the Requester must demonstrate that the Board (or in this case the NGPC) failed to consider material information or considered false or inaccurate material information in adopting the Resolution. (Bylaws, Art. IV, § 2.2.) The Requester does not argue that the NGPC considered false or inaccurate material information, but it does claim that the NGPC failed to consider material information in two ways. First, the Requester claims that the NGPC did not sufficiently consult with the public prior to adopting the Resolution. Second, the Requester claims that the NGPC failed to consider how the Resolution will have material adverse effects on registries and internet users. Neither argument withstands scrutiny, and neither is grounds for reconsideration.

1. The NGPC Considered Public Comments Solicited During A Lengthy Public Comment Period.

The Requester claims the NGPC "failed to take material input from the community into account." (Request, § 8, Pg. 11.) Contrary to the Requester's claims, however, the NGPC did

[28] The Requester states that it sent a letter to the NGPC "well in advance" of the NGPC meeting, but that statement is wrong given the mere three days between the date of the letter and the 30 July 2014 NGPC meeting. (*See* Request, § 8, Pg. 9.)

consider feedback received in "the public comment forum"[29] that was open from 26 February 2014 through 21 April 2014. The Requester does not explain why it declined to participate in that forum. Had it participated, its views would have been included along with the 28 detailed comments that were submitted by various stakeholders and members of the public, including other registries.[30] The Resolution expressly notes that the NGPC took into account the 28 comments received via the forum.[31] The Requester cannot reasonably claim, then, that the NGPC did not consider public input before adopting the Resolution. The Requester nonetheless complains that "the community-at-large were [*sic*] allowed to provide input until April 21, 2014, but not after that date." (Request, § 8, Pg. 11.) Notably, however, the public comment period for this matter was actually longer than is required. Typically, public comment periods are open 21 days, and if comments are received during that time, there is a 21-day reply period.[32] Here, the public comment period was open for 33 days, with a 21-day reply period. Moreover, ICANN facilitated an entire public session about the name collision issue at the London ICANN meeting on 23 June 2014 that provided yet another opportunity for public commentary and participation; the Requester again chose not to participate.[33]

In sum, the Requester does not persuasively argue that the NGPC failed to consider material information in the form of public comments in adopting the Resolution, and therefore has not stated proper grounds for reconsideration on that basis. (Bylaws, Art. IV, § 2.2.)

---

[29] *See* Resolution, *available at* https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf.
[30] *See* Report of Public Comments, *available at* https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf.
[31] *See* Resolution, *available at* https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en.
[32] *See* https://www.icann.org/resources/pages/how-2014-03-17-en
[33] *See* Name Collision Presentation, London: ICANN 50, *available at* https://london50.icann.org/en/schedule/mon-name-collision/presentation-name-collision-23jun14-en.

2. The NGPC Considered All Material Information Relevant To The Resolution.

The Requester seeks reconsideration of the Resolution because it claims the NGPC "did not properly assess the implications of the decision." (Request, § 8, Pg. 12.) The Requester's main basis for this assertion is that the issues raised in its own 27 July 2014 letter were not expressly addressed in the "Rationale" section of the Resolution. This argument fails to provide a basis for reconsideration for two reasons.

First, the Resolution *does* take into account the substance of the information provided in the Requester's 27 July 2014 letter; the NGPC simply reached a different conclusion than the Requester as to what the proper solution to name collision issues should be. The 27 July 2014 letter made five requests, all related to either the "RPM rules" or the Requester's view that one common set of rules should apply to all gTLDs. (Request, § 8, Pg. 10 & Ex. D.) Despite Requester's claims of disregard, the same issues raised in the 27 2014 July letter were all presented to the NGPC during the public comment period by other stakeholders and were addressed by the NGPC. The Resolution acknowledges that the community expressed – during the public comment period – concerns regarding the "interaction between the name collision block lists and intellectual property rights protection mechanisms."[34] The NGPC also indicated that it considered the public comments that reference how the "name collision issue is creating an uneven competitive landscape" as well as other public comments that discussed the pros and cons of treating new gTLD operators differently from legacy operators.[35] And, finally, ICANN has already determined that the RPM issue requires further public comment before a decision can

[34] *See* Resolution, *available at* https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf.
[35] *See* Report of Public Comments, at Pg. 11, *available at* https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf.

be made as to how to handle the issue. In fact, ICANN is currently soliciting comments, between 25 August 2014 and 7 October 2014, on the approach that should be taken "regarding the appropriate Rights Protection Mechanisms for release of SLD Block List names."[36] In other words, the NGPC was not lacking any material information on the applicable issues, regardless of whether it specifically considered the Requester's 27 July 2014 letter.

Second, the Requester's disagreement with the substance of the Framework does not form the proper basis for reconsideration; here, only if the NGPC adopted the Resolution "without consideration of material information" is reconsideration warranted. (Bylaws, Art. IV, § 2.2.) As the Resolution makes clear, the NGPC considered independent, detailed studies discussing the name collision issue, including one prepared by JAS and one prepared by Interisle Consulting Group (which was in response to advice from the SSAC).[37] Further, the NGPC took into account advice from the SSAC before adopting the Resolution. The SSAC's role is to "advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems." (Bylaws, Art. XI, § 2.a.) In sum, the NGPC considered public comments, independent analytical reports, and advice from the relevant ICANN advisory committee. While the Requester complains that the NGPC "did not mention the letter" (that the Requester sent months after the public comment period had closed) and as such "did not properly address the implications of the decision" to approve the Framework, those allegations do not amount to a claim that the NGPC failed to consider any material information. As such, no reconsideration is warranted.

[36] *See* Implementing Rights Protection Mechanisms in the Name Collision Mitigation Framework, *available at* https://www.icann.org/public-comments/name-collision-rpm-2014-08-25-en
[37] *See* Resolution, *available at* https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-07-30-en.

As a final note, the Requester also claims reconsideration is warranted because "[t]here is no indication that the GAC[38] has been given the opportunity to provide feedback" to the JAS reports or the SSAC advice. (Request, § 7, Pg. 7) The GAC provides "advice on the activities of ICANN as they relate to concerns of governments, particularly matters where there may be an interaction between ICANN's policies and various laws and international agreements or where they may affect public policy issues." (Bylaws, Art. XI, § 2.1.) That the GAC did not issue any formal advice related to how ICANN should address name collisions does not mean the NGPC failed to consider any material information. Had the GAC issued such advice, the ICANN Board would have considered it, as is required under ICANN's Bylaws. (Bylaws, Art. XI, §§ 2.1.i, 2.1.j.) Further, in July 2013, the GAC Durban Communiqué did advise that the Board "[a]s a matter of urgency consider the recommendations contained in the SSAC Report on Dotless Domains (SAC053) and Internal Name Certificates (SAC057)," and the latter involved name collision issues.[39] The Board did consider the SSAC's advice, and in turn, put the Framework in place.

Once again, because the Requester does not persuasively argue that the NGPC failed to consider material information in adopting the Resolution, it has not stated proper grounds for reconsideration. (Bylaws, Art. IV, § 2.2.)

C. Reconsideration Is Not Warranted On the Grounds That The Requester Or Others Might Be Confused By The Framework.

The Requester complains that the NGPC failed to consider the supposed fact that the "overall majority" of registrants are not aware of the name collision problem and will therefore be "confus[ed] about the availability of domain names in general." (Request, § 7, Pg. 6.)

[38] Government Advisory Committee.
[39] *See* GAC Communiqué Issued at ICANN 47, *available at* https://www.icann.org/news/announcement-2013-07-18-en; SAC057, *available at* https://www.icann.org/en/system/files/files/sac-057-en.pdf.

However, the NGPC clearly did consider information concerning the importance of educating the public about the Framework, because the Resolution dedicates an entire provision (section B.6) to "Informational Materials" and requires ICANN to "produce informational materials as needed . . . . [and] work to make this information available to parties potentially affected by name collision."[40] Even though the Framework was adopted less than one month ago, ICANN has already posted on its website a wide variety of informational materials, including webinars geared towards registry operators, handbooks and videos for IT professionals, and a "Frequently Asked Questions" page regarding the Framework.[41] Moreover, ICANN has dedicated resources towards ensuring questions about the Assessment or the Framework will be answered promptly and accurately. In other words, far from failing to consider the potential for confusion regarding the Resolution, the NGPC and ICANN have taken proactive and significant steps to ensure that affected members of the public, and in particular the registries, comprehend the Framework and the steps it requires.[42] No reconsideration is warranted on the grounds that the NGPC did not consider information regarding public outreach, as it is clear the NGPC did consider such information and acted on it by way of the aforementioned educational resources.

D. The Requester Has Not Demonstrated It Has Been Materially Affected By The Resolution.

Absent evidence that the Requester has been materially and adversely affected by the Resolution, reconsideration is not appropriate. (Bylaws, Art. IV, §§ 2.1-2.2.)

---

[40] *See* Resolution, *available at* https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf.
[41] *See* Name Collision Resources & Information, *available at* https://www.icann.org/resources/pages/name-collision-2013-12-06-en.
[42] ICANN has also engaged in significant outreach activities on LinkedIn and via various media outlets, as well as launching a Google Adwords promotion.

Here, the Requester argues it is materially affected by the Resolution for two reasons. (Request, § 6, Pgs. 4-5.) First, it contends that the Framework does not provide clear guidance as to how to prevent harms related to name collisions. (*Id*., Pg. 5.) Second, the Requester contends that it will suffer "lower registration rates" due to the confusion the Framework will purportedly cause, because the Requester predicts that registrars will "not offer domain name registrations from the Name Collision lists." (*Id*.) Neither of these concerns has yet come to fruition, however, and are merely speculative at this point. Again, only those persons who "*have been* adversely affected by" an ICANN action may file a request for reconsideration. (Bylaws, Art. IV, § 2.2) (emphasis added). Because the only harm the Requester identifies is, at this point, merely speculative and hypothetical, the request for reconsideration is premature.[43]

As such, the Requester has failed to demonstrate it *has been* materially affected by the Resolution and, on that independent basis, reconsideration of the adoption of the Resolution is not warranted.

VI. Determination.

Based on the foregoing, the BGC concludes that the Requester has not stated proper grounds for reconsideration, and therefore recommends that Reconsideration Request 14-37 be denied.

[43] In fact, the Framework will permit names to be activated in the DNS now that were previously not allowed to be activated. As such, the Framework may well lead to an increase in registrations.

Clarification to Reconsideration Request 14-37

The Board Governance Committee stated in their minutes to Reconsideration Request 14-37, to our answer provided in **Question 6. Describe how you believe you are materially affected by the action or inaction:**

> *First, it contends that the Framework does not provide clear guidance as to how to prevent harms related to name collisions. (Id., Pg. 5.) Second, the Requester contends that it will suffer "lower registration rates" due to the confusion the Framework will purportedly cause, because the Requester predicts that registrars will "not offer domain name registrations from the Name Collision lists." (Id.) Neither of these concerns has yet come to fruition, however, and are merely speculative at this point. Again, only those persons who "have been adversely affected by" an ICANN action may file a request for reconsideration. (Bylaws, Art. IV, § 2.2) (emphasis added). Because the only harm the Requester identifies is, at this point, merely speculative and hypothetical, the request for reconsideration is premature.*
>
> *As such, the Requester has failed to demonstrate it has been materially affected by the Resolution and, on that independent basis, reconsideration of the adoption of the Resolution is not warranted.*

We would like to provide the BGC and NGPC with more details how we already are and still will be materially affected. Those details derive from our two TLDs, which are in operations since January 2014.

We receive inquiries on a daily basis from registrars, resellers and registrants whether domain names can be registered and if not, when they will become available for registration. We would like to provide you with an excerpt:

1. Inquiries by registrars
    a. MarkMonitor (March 13, 2014): blogger, wordpress, yahoo
    b. MarkMonitor (April 17, 2014): facebook
    c. CSC (July 15, 2014): „Can you please confirm if registration of domains on ICANN's NXD list is permitted during GA for .rich and .onl?"
    d. Inquiring registrars: Among others MArkMonitor, Marcaria, CSC, Ascio / NetNames, Nom-IQ d.b.a. Com Laude, Safenames, Nameshield, 101domain, Superregistry, OpenProvider and united-domains.

2. Inquiries by registrants
    a. Google inquiry for: youtube, gmail, google
    b. Direct inquiries for poker.onl, casino.onl, email.onl, games.onl, filthy.rich, super.rich and the.rich.
    c. Inquiries by major domain investors (names can be provided on request).

3. Statistics from our backend about unsuccessful attempts to register a domain due to Name Collision:
    a. For example: 23 Name Collision Domains received 1.468 failed attempts to register the domain.
    b. The domain names are: wedding, vitamins, sports, shop, seo, search, realestate, porn, poker, news, mobile, login, image, health, games, game, forex, facebook, edu, cars, car, app, 888.
    c. Most of these domain names would have been sold as premium names.

The overall experience we hear from registrants is that the process is very heterogeneous, inconsistent and untransparent. Registrants cannot be sure to get the same result nor a correct result for the same domain name across registrars:

- Only a few registrars synchronized their databases with the name collision list and do provide end users with the result.
- Some registrars keep this process manual and inquire with us.
- Some registrars give the status, that the domain name is “already registered“ or “not available”.

As a result, there is no reliability for registrants, they are confused by the diverse statements by different registrars about the same domain name. They refrain to register the respective domain name – as we can see from our zone file.

A simple, unified process where and how to register Name Collision domain names is the key element for registrants, registrar and registries.

As long as clear rules and guidance are missing, this pattern of confusion will go on and continue to harm us materially.

We would also like to clarify that we are already affected materially right now: Those effects described above are important criteria in determining the possible revenues and thus the value of the string and the auction price. Our Investors determined that the value of .VIP is lower in comparison to TLDs without the Name Collision issue and thus they valued .VIP now roughly 20% lower than they did before the Name Collision effect appeared. In return they claim higher interest and securities which cause proportionately higher costs on our side.

September 11, 2014

sgd. Anschelika Smoljar

I-REGISTRY Ltd.

SAC057
SSAC Advisory on Internal Name Certificates

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
15 March 2013

Preface

This is an advisory to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning security and stability implications for internal name certificates. The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this advisory, references to SSAC members' biographies and statements of interest, and SSAC members' objections to the findings or recommendations in this advisory are at end of this advisory.

Table of Contents

Executive Summary

The SSAC has identified a Certificate Authority (CA) practice that, if widely exploited, could pose a significant risk to the privacy and integrity of secure Internet communications. This CA practice could impact the new gTLD program. The SSAC thus advises ICANN take immediate steps to mitigate the risks.

1. Introduction

Certificate Authorities, also known as Certification Authorities, (CAs) are organizations that issue digital certificates. These digital certificates certify the ownership of a public key by the named subject of the certificate. This allows others to rely upon signatures or assertions made by the private key that corresponds to the certified public key.

The CAs typically validate the identities of requestors before they issue certificates. For example, when Internet users browse to https://www.myicann.org/, their browsers know it is the real myicann.org because GoDaddy, a CA, has vouched the registered holder of myicann.org and issued a certificate to it. This system breaks down, however, if CAs are unable to validate the applicants they vouch for and their authority over the domain name for which the certificate is applied.

One such instance is the "Internal Name" certificate (also known as "non-fully qualified domain names" or non-FQDNs). An Internal Name certificate contains a name that is not currently resolvable using the public Domain Name System (DNS) and which is assumed to be for private use only.

An internal name is a domain or Internet Protocol (IP) address that is part of a private network. These internal names are not allocated to any specific organization and therefore cannot be verified. Common examples of internal names are:

- Any server name with a non-public domain name suffix. For example, www.company.local or server1.company.corp.
- NetBIOS names or short hostnames, anything without a public domain. For example, Web1, ExchCAS1, or Frodo.
- Any IP address in the RFC1918[1] range. These addresses are reserved for private networks only.

Internal names are not verifiable by CAs because it is not possible to look up who owns them. When determining whether a certificate application is for internal use or not, CAs often rely on the list of currently delegated Top Level Domains (TLDs) and not, for instance, against the list of the TLDs applied for in ICANN's new Generic TLD (gTLD) program. For instance, although `www.exampletld` is currently an internal name,

[1]Note: RFC 1918 is updated by RFC 6761.

`exampletld` could be an applied-for-TLD and `www.exampletld` may later become operational.

In this advisory, the SSAC examines the prevalence of internal name certificates, analyzes the security risk it imposes, and advises ICANN to take a few mitigation steps. The SSAC also wishes to highlight that although this practice has immediate impact to new gTLDs, it has larger security ramifications.

2. SSAC Preliminary Research

2.1 Empirical Analysis

The SSAC performed analysis with data from the Secure Sockets Layer (SSL) Observatory to examine the prevalence of internal name certificates and their potential for impact to ICANN's new gTLD program.

The SSL Observatory is a project sponsored by the Electronic Frontier Foundation (EFF) to investigate the certificates used to secure sites encrypted with Hypertext Transfer Protocol Secure (HTTPS) on the Web. The dataset contains all of the publicly visible SSL certificates on the Internet Protocol Version 4 (IPv4) Internet as of August 2010.[2]. The observatory data is made available as a My Structured Query Language (MySQL) database and contains 1,377,067 unique valid certificates signed by 1,482 certificate authorities.

The SSAC notes that in the EFF dataset, the term "certificate authorities" means roots and intermediate authorities used to issue certificates. So, although many of these are controlled by the same organization, the EFF dataset treats them as different entities. In reality, there are about 70 organizations that control the issuance of these certificates.

According to security researchers,[3] in total there are 37,244 internal name certificates issued by 157 CAs, 2.7 percent of all the public certificates available in the SSL repository. The top 10 certificate authorities that issue internal name certificates are:

Table 1: Top 10 Issuers of internal name certificates. Data Source: SSL Observatory

Number of non-FQDN certs issued	Issuer
11615	Go Daddy Secure Certification
6663	Positive SSL CA
4807	DigiCert Hi Assurance CA-3
1967	Starfield Secure Certification Authority
1731	AAA Certificate Services

[2]See The EFF SSL Observatory Project at: https://www.eff.org/observatory.
[3]See https://www.eff.org/deeplinks/2011/04/unqualified-names-ssl-observatory.

1520	DigiCert Global CA
1155	USERTrust Legacy Secure Server CA
930	GlobalSign Domain Validation CA
889	Equifax Secure Certificate Authority
799	Entrust Certification Authority

The SSAC queried the SSL observatory for internal name certificates that ends in an applied for TLD string. There are 1,053 such certificates that end in 63 applied-for TLD strings. Among those, 210 have not expired and are therefore still valid and working.

In the following example, we show a valid internal name certificate that conflicts with an applied for gTLD, .corp.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:02:c2:90:e4:43:22
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc.,
OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure
Certification Authority/serialNumber=07969287
        Validity
            Not Before: Dec 22 10:07:40 2009 GMT
            Not After : Jan  8 22:08:22 2013 GMT
        Subject: O=webmail.quiksilver.com.au, OU=Domain Control
Validated, CN=webmail.quiksilver.com.au
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)

            X509v3 Subject Alternative Name:
                DNS:webmail.quiksilver.com.au,
DNS:www.webmail.quiksilver.com.au, DNS:owa.quiksilver.com.au,
DNS:autodiscover.quiksilver.com.au, DNS:webmail.dcshoes.com.au,
DNS:webmail.dcaus.com, DNS:qsauhub01,
DNS:qsauhub01.sea.quiksilver.corp, DNS:qsauhub02,
DNS:qsauhub02.sea.quiksilver.corp, DNS:autodiscover.sea.quiksilver.corp
```

Figure 1: A certificate that has internal names that end in an applied for TLD string.

The above certificate was issued to webmail.quiksilver.com.au. However, it is also valid for qsauhub01, qsauhub01.sea.quiksilver.corp, qsauhub02, qsauhub02.sea.quiksilver.corp, and autodiscover.sea.quiksilver.corp.

This is due to a known feature called "Subject Alternative Names" in X.509 certificates. A Subject Alternative Name is an attribute that lists an alternate name for the subject of the certificate. In a web context that subject is the hostname. This functionality provides SSL-secured communication for servers using multiple domain names and host names – within a single SSL certificate. In the example above, the certificate is also valid for qsauhub01.sea.quiksilver.corp, qsauhub02.sea.quiksilver.corp, and autodiscover.sea.quiksilver.corp, all of which end in the applied for TLD string "corp".

Limitation of the empirical analysis: The SSAC notes that, due to the following reasons, the above analysis could *significantly* undercount the number of internal name certificates that collide with ICANN's applied-for-TLD string.

1) The SSL observatory database only contains publicly available certificates on the IPv4 network. Its methodology is not capable of discovering internal certificates that are not associated with a public certificate. Since the key purpose for internal name certificates is for internal use, it is highly likely that many internal certificates are unaccounted for.

2) It is also possible that the SSL observatory is not scanning ports typically used with mail servers. Many certificates with internal server names are used to secure these systems, therefore undercounting the number of such certificates.

3) The dataset is from 2010.

2.2 Case Study

The SSL observatory data dates back to 2010. To examine whether it is still possible today to register internal name certificates, an SSAC member tried to obtain an internal name certificate (www.site) that ends in an applied for TLD string (.site) in the fourth quarter of 2012. This section outlines the steps he took to obtain the certificate.

Step 1: Request – The researcher created a certificate-signing request (CSR) for www.site. Additional details of the request are listed below.

```
Data:
Version: 0 (0x0)
Subject: C=US, ST=XX, L=XXXX,
O=XXXXXX,
OU=IT - Internal WWW Site.,
CN=www.site/emailAddress=XXXX@XXXX.net
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:da:ef:bd:d0:ee:db:.. (omitted)
```

Figure 2: Certificate Request for www.site. "SITE" is currently an applied for TLD in ICANN's new gTLD program. The contact information of the requester is redacted for privacy purposes.

Step 2: Interaction with the CA – The CA detected that www.site is not a fully qualified domain name, and asked the requester to confirm it is intended for internal use.

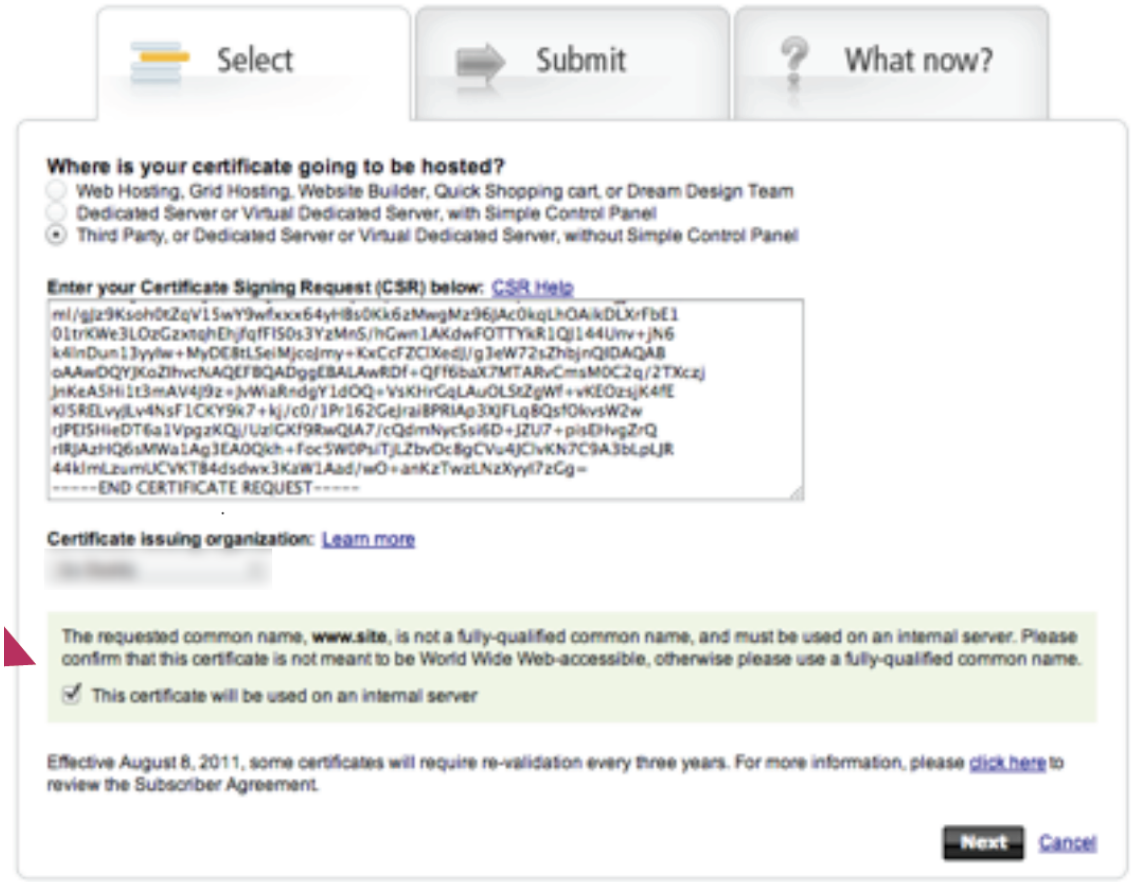


Figure 3: Interaction with CA. The boxed content says, "The requested common name, www.site, is not a fully-qualified common name, and must be used on an internal server. Please confirm that this certificate is not meant to be World Wide Web-accessible, otherwise please use a fully qualified common name. [check box] This certificate will be used on an internal server.

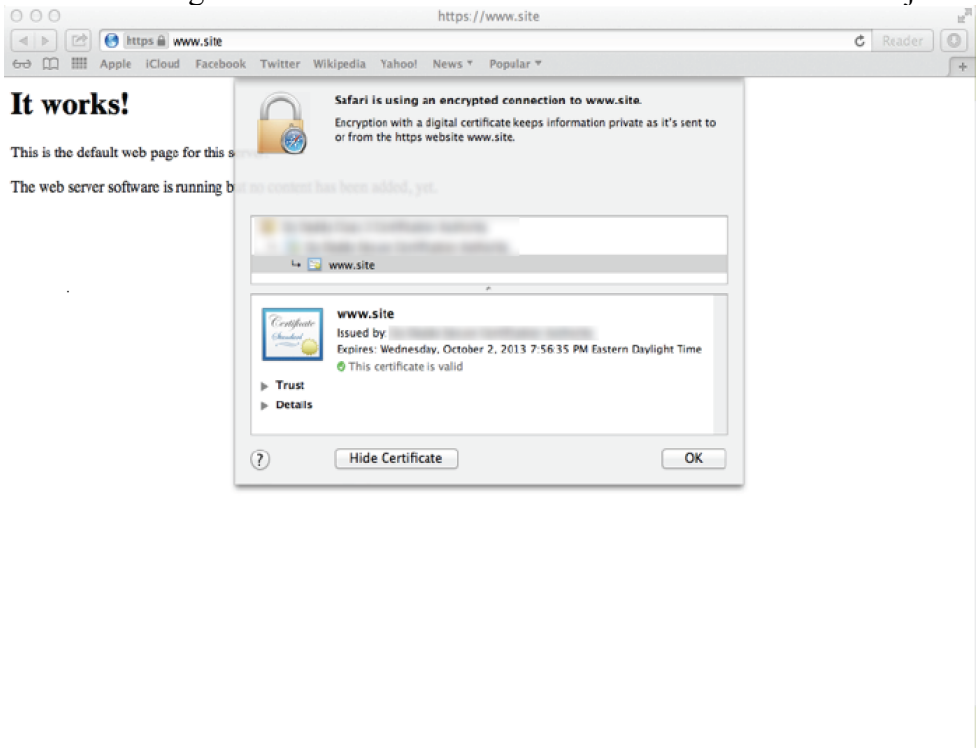
Step 3: Certificate Issued – After the researcher confirmed that he understood that this is for internal use the CA issued a certificate valid for one year. Additional details of the certificate are listed below.

```
Version: 3 (0x2)
Serial Number: 27:e7:22:63:59:11:b0
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=XXX, L=XXX, O=XXX, OU=XXX,
CN=XXX/serialNumber=XXXXXXXX
Validity
Not Before: Oct 2 23:56:35 2012 GMT
Not After : Oct 2 23:56:35 2013 GMT
Subject: O=www.site, OU=Domain Control Validated,
CN=www.site
X509v3 Subject Alternative Name:
DNS:www.site, DNS:site
```

Figure 4: Certificate issued by the CA. The name of the CA is redacted for security reasons.

Step 4: Verification – The SSAC member set up www.site[4] and verified that various

Browsers recognize the certificate. Below is a screenshot from one major browser.



[4]Using a "fake" / local root with .site delegated.

3. Findings

Based on the preliminary research above, the SSAC offers the following findings.

Finding 1: The SSL observatory data shows that at least 157 CAs have issued internal name certificates. If these practices do not change, any of them could issue certificates that end in an applied for new gTLD. Our case study shows that as of this writing this is possible with at least one CA.

Finding 2: The exact number of internal name certificates that end in an applied for new gTLD cannot be known unless CAs voluntarily disclose the list.

The SSL observatory database only contains certificates that were publicly visible (could be found by probing port 443 from the Internet). There could be many certificates issued that are only used internally and would not have been visible to the SSL observatory project. Thus there is no way of knowing how many of those certificates exist unless certificate authorities voluntarily disclose them.

Finding 3: Enterprises use internal name certificates for a variety of reasons.

According QuoVadis Group, a certificate authority, one use case for internal name certificate is for convenience:

> As a convenience for users, many servers in corporate networks are reachable by local names such as "mail", "wiki" or "hr". Most publicly trusted certificates for non-unique names are deployed in the context of local networks to enable trust in these local names without the additional cost of provisioning a new trust root to clients. This may be especially desirable for networks lacking centralized policy deployment and management tools, such as "Bring Your Own Device" environments.[5]

As shown in our empirical analysis, there are at least 37,000 internal name certificates used in thousands of enterprises. Although this practice *might* make sense in the previous two autonomous systems (DNS and CAs), with the introduction of new gTLDs, namespace collisions and other man-in-the-middle attacks (see Finding 4) will become more apparent. In addition, because many of the applied for TLDs are common, generic terms the risk of collisions increases.

[5]See QuoVadis Group. 2012. Internal Server Names and IP Address Requirements for SSL at: https://support.quovadisglobal.com/AvatarHandler.ashx?radfile=%2fCommon%2fSSL+General+Topics+%28KB%29%2fQV_DeprecatedCertsGuidance_v2.pdf.

Finding 4: The practice for issuing internal name certificates allows a person, not related to an applied for TLD, to obtain a certificate for the TLD with little or no validation, and launch a man-in-the-middle attack more effectively.

If an attacker obtains a certificate before the new TLD is delegated, he/she could surreptitiously redirect a user from the original site to the attacker site, present his certificate and the victim would get the Transport Layer Security/SSL (TLS/SSL) lock icon. This poses a significant risk to the privacy and integrity of HTTPS communications as well as other protocols that use X.509 certificates (e.g. TLS/SSL-based email communication).

To date, at least two security researchers have confirmed this is possible. In both cases, they were able to obtain certificates for applied-for new gTLDs.

Finding 5: The CA / Browser (CA/B) forum is aware of this issue and requests its members to stop this practice by October 2016. The vulnerability window to new gTLDs is at least 3 years.

In the "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates" that went into effect on 1 July 2012, the CA/B forum states that:

> As of the Effective Date [1 July 2012] of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date [1 July 2012], the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.[6]

Although this is welcome news, this is still *problematic* because ICANN plans to delegate new TLDs in 2013, introducing vulnerability for potential new gTLDs until October 2016.

[6]CA/Browser Forum. Baseline Requirements for the Issurance and Management of Publicly-Trusted Certificates, v. 1.0. 22 November 2012. Available at: https://www.cabforum.org/Baseline_Requirements_V1.pdf.

4. Recommendation

Recommendation: The ICANN Security Team should immediately develop and execute a risk mitigation plan.

The mitigation plan should include at least:

- Outreach to the CA/B forum[7] and CAs, requesting that they treat applied for new gTLDs as if they were delegated TLDs as soon as possible, as well as discussing the broader implications and mitigation steps.

  In doing so, ICANN should seek to create trust relationships between ICANN and CA/B Forum and CAs. Because of the potential for collateral harm to users if disclosure is made public before mitigation is effected, the SSAC believes it is important to conduct correspondence confidentially.

- A Disclosure Policy as informed by industry best practices for vulnerability disclosure (e.g. CERT / CC vulnerability disclosure.[8] Such a policy should take into consideration that once the disclosure is public, it is trivial to exploit the vulnerability.

- A communication plan on informing affected parties as determined by the disclosure policy.

- A contingency plan to be executed if the vulnerability is leaked to the public prematurely, as well as a proactive vulnerability disclosure plan.

5. Acknowledgments, Statements of Interests, and Objections and Withdrawals

In the interest of greater transparency, these sections provide information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

[7]See Certificate Authority / Browser Forum: https://www.cabforum.org. As of the publication of this advisory the outreach is already in progress.

[8]See CERT/CC. CERT/CC Vulnerability Disclosure Policy at: http://www.cert.org/kb/vul_disclosure.html.

5.1 Acknowledgments

The committee wishes to thank the following SSAC members and external experts for their time, contributions, and review in producing this advisory.

SSAC members

Steve Crocker
Patrik Fältström
Ondrej Filip
James Galvin
Warren Kumari
Danny McPherson
Ram Mohan
Doron Shikmoni

ICANN staff

Jeff Moss
Dave Piscitello
Barbara Roseman
Steve Sheng (editor)

During the production of this advisory, the SSAC reached out to the certificate authority community to get feedback. For their time and contributions during this outreach process, the SSAC wants to specifically thank the following persons/organizations:

Certificate Authority Browser Forum (CA/B Forum)
Certificate Authority Security Council (CASC)
Ben Wilson (Digicert)
Jeremy Rowley (Digicert)

5.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/groups/ssac/biographies-01feb13-en.htm..

5.3 Objections and Withdrawals

There were no objections or withdrawals.

Appendix A: SSAC Publication of This Advisory and Chronology of Mitigation

Due to the sensitive nature of this issue, the SSAC did not follow its customary publication procedures; instead, the SSAC delivered an interim advisory to the ICANN Security Team. The ICANN Security Team took immediate action. This section, jointly contributed by the ICANN Security Team, provides a chronology of events related to the mitigation of this risk as of the time of publication of this advisory.

SSAC Advisory Formation: During its annual workshop on 14 – 16 November 2012, a SSAC member presented to the SSAC the process he used to register an internal name certificate that ended in an applied-for-gTLD string. Recognizing the seriousness of this issue, the SSAC formed a work party to develop some advice for ICANN. The work party met weekly from 30 November to 17 December and produced a first draft of this advisory.

On 8 January 2013, a briefing call was conducted between SSAC work party members and staff from ICANN's Security Team and Legal Department. During that call, ICANN agreed to start preparing mitigation options in anticipation of the SSAC advisory.

On 19 January 2013, the SSAC work party finished its work on the internal name certificate advisory, and sent the advisory for full SSAC review.

On 28 January 2013. The SSAC completed the review of the advisory. During the SSAC deliberation, the best path of disclosure became an issue of active discussion. It was apparent that 1) this information is not widely exploited yet, and if leaked could lead to security attacks, 2) no means to mitigate the problem exist at this time. Thus the SSAC decided to send the advisory to the ICANN Security Team first to give them an opportunity to act on the mitigation plan recommendation, and requested ICANN keep this advisory confidential until otherwise directed by the ICANN Chief Security Officer. The Chief Security Officer (or his/her authorized delegate) would approve and record selected release of the advisory to appropriate individuals and would judge when confidentiality is no longer warranted, informed by the recommended mitigation plan.

On 31 January 2013, the SSAC submitted the advisory to the ICANN Security Team.

ICANN and CA/Browser Coordinated Mitigation: Shortly after 8 January briefing, ICANN formed a risk mitigation team composed of staff from policy, security, new gTLD and DNS industry engagement. The team held regular meetings to plan the mitigations.

On 23 January 2013, the ICANN Security Team scheduled a preliminary teleconference with the Certificate Authority and Browser Forum (CA/B) Chairperson to alert him of this issue. Recognizing the seriousness of this issue, the chairperson invited ICANN to brief the CA/B forum members in its upcoming annual meeting.

On 5 February 2013, ICANN presented the SSAC advisory to the CA/B Forum annual meeting and re-iterated its commitment to work with CAs and Browsers to address this issue. As a result of this meeting, the CA/B Forum advanced Ballot 96 on new gTLDs. The ballot called for CAs to stop issuing certificates that end in an applied-for-gTLD string within 30 days of ICANN signing the contract with the registry operator, and revoke any existing certificates within 120 days of ICANN signing the contract with the registry operator *[NOTE: the original CA timeline for not issuing internal name certificates was 1 July 2015, with revocation starting on 1 October 2016]*. The full text of the ballot is included as Appendix B to this document. The voting period for this ballot started at 21:00 UTC on 13 February 2013 and closed at 21:00 UTC on 20 February 2013.

Responding to some questions on the ballot, on 15 February 2013 ICANN provided the following statement to the CA/B Forum:

> "All current registry agreements are published at the following URL: https://www.icann.org/en/about/agreements/registries. New gTLD registry agreements will be published to this page as they become available. In addition, ICANN plans to implement a notification or web feed for the items on this page. If this URL should change, ICANN will notify visiting users of the new location of the registry agreements.
>
> ICANN is willing to work with the CA/B forum, and other interested parties, to understand additional notification needs."

On 20 February 2013, the CA/B Forum passed Ballot 96 (Wildcard certificates and new gTLDs) with 14 in favor, 2 opposed, and 4 abstentions.

On 12 March 2013, the SSAC finalized its advisory based on the mitigations and additional input provided by the Certificate Authority Security Council.

The SSAC commends the ICANN security team and CA/B forum for its timely attention and mitigation of this risk, and requests ICANN to continue work with CAs, browser developers and other relevant parties to further mitigate the risk.

Appendix B: CA/B Forum Ballot 96

... Motion Begins ...

... Erratum Begins ...

Add the following as new Section 11.1.3:

11.1 Authorization by Domain Name Registrant

11.1.3 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure† that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled† or public suffix, CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

Prior to September 1, 2013, each CA MUST revoke any valid certificate that does not comply with this section of the Requirements.

†Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as http://publicsuffix.org/. If the process for making this determination is standardized by an RFC, then such a procedure SHOULD be preferred.

Add the following as new Section 11.1.4:

11.1.4 New gTLD Domains

CAs SHOULD NOT issue Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal Server Name with a gTLD that ICANN has announced as under consideration to make operational, the CA MUST provide a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA will revoke the Certificate unless the applicant promptly registers the domain name.

Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.icann.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after

the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 11.1.

Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

... Erratum Ends ...

The review period for this ballot shall commence at 21:00 UTC on 6 February 2013 and will close at 21:00 UTC on 13 February 2013. Unless the motion is withdrawn during the review period, the voting period will start immediately thereafter and will close at 21:00 UTC on 20 February 2013. Votes must be cast by posting an on-list reply to this thread.

... Motions ends ...

Details

ICANN

Announcements

05 Aug 2013

New gTLDs
SSR
Security
gTLD

Addressing the Consequences of Name Collisions

As directed by the ICANN Board of Directors on 18 May 2013, ICANN commissioned and today releases the results of a study that considers the likelihood and impact of name space collisions between applied-for new gTLD strings and non-delegated TLDs. Additionally, the study also reviewed the possibility of collisions arising from the use of X.509 digital certificates.

Background: In a study published in January 2013, ICANN's Security and Stability Advisory Committee (SSAC) identified fact that some certificate authorities issue X.509 certificates for domain names that are not resolvable in the public DNS. Such issues identified in SAC 057, as well as in SAC 045, are symptoms of entities that have local environments that include strong assumptions about the number of top-level domains and/or have introduced local top-level domains in private namespaces that may conflict with names yet to be allocated. These private namespaces sometimes "leak" into the public DNS (either through misconfiguration or the use of old

software), meaning that requests for resources on private networks could end up querying the public-facing DNS Root Servers and hence "colliding" with the delegated new gTLD.

The Study: On 18 May 2013, the ICANN Board approved a resolution calling for a detailed study of the name collision issue. ICANN contracted with Interisle Consulting Group, LLC to collect and analyze the necessary data on all applied-for strings.

The resulting study, *Name Collision in the DNS* [PDF, 3.34 MB], identifies three categories of strings by the potential risk of name space collision:

- **Low Risk:** 80% of applied-for strings.
- **Uncalculated Risk:** 20% of applied-for strings.
- **High Risk:** 2 strings (.home, .corp).

To minimize the likelihood of any impact, ICANN proposes to the community several mitigation measures to be taken as described in an accompanying staff recommendation paper, *New gTLD Collision Risk Management* [PDF, 166 KB]. They include:

- Proceeding with contracting and delegation of those strings categorized as **"low risk" (80%)** but recommending additional mitigation measures which should not materially impact their timeline for delegation.
- Conducting further study on those strings categorized as **"uncalculated risk" (20%)** anticipated to take 3-6 months to complete.
- Delaying contracting and delegation of the two **"high risk"** strings until mitigation efforts can place them in the "low risk" category.

New gTLD Security and Stability: Throughout the development of the New gTLD program, the security and stability of the Domain Name System has remained the paramount concern of the ICANN community. ICANN staff has

prepared an information sheet, *Secure and Stable Introduction of new gTLDs* [PDF, 102 KB], that describes the measures ICANN has taken to ensure the introduction of new gTLDs will not jeopardize that commitment.

Public Comment: At this time, the mitigation steps outlined in the staff recommendation paper are proposals only and community input is strongly suggested. As a result, ICANN has opened a formal process for soliciting public comment. The form for submitting public comment and the calendar for doing so is available here.

Coordinated Vulnerability Disclosure Process: ICANN takes this opportunity to inform the community that it has updated its risk management procedures for improved reporting and response to any unforeseen issues arising from the delegation of new gTLDs. Members of the community are urged to familiarize themselves with the process available for review here [PDF, 628 KB].

More Announcements

ICG Considering Future Meeting Requests from Community

IDN ccTLD Request from the Republic of Belarus Successfully Passes String Evaluation

Call for Observers to Join Cross Community Working Group to Develop an IANA Stewardship Transition Proposal on Naming Related Functions

Chinese Community Steps Forward for Chinese TLDs - Forms Generation Panel for Root Zone Label Generation Ruleset (LGR)

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.

Mitigating the Risk of DNS Namespace Collisions

A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation

Phase One Report

4 JUNE 2014

TABLE OF CONTENTS

1 Discussion of Public Comments and Revisions

JAS would like to sincerely thank all of the individuals that have participated in the review and comment process. We received significant and valuable feedback from the public draft and numerous other discussions since the initial release of our document in February. We have amended our report accordingly. Specifically, we have addressed the following issues:

- Discussion of IPv6-related issues (see new Section 3.1.3);
- Recognition of emergent data and experience (see new text in Section 2);
- Additional discussion concerning the implementation tradeoffs of using a 127/8 IP vs. an Internet IP ("Honeypot") for Controlled Interruption (see additions to Section 3.1.7);
- Reduction of Controlled Interruption period to 90 days (see new Section 3.1.2);
- Additional description of our findings regarding probability and severity of possible impacts resulting from name collision occurrences (see new text in Section 3.1.6);
- Discussion of staggered vs. consistent introduction of Controlled Interruption (see new text in Section 3);
- Recommendation to collect additional logs to support long-term measurement of the collisions phenomena (see new text in Section 3.2);
- Description of content that is expected to appear in our Phase Two report (see new section 3.4); and
- Other minor modifications, improvements, and elaborations throughout.

2 Summary and Preface to Phase One Report

Collisions in the global Domain Name System (DNS) namespace have the potential to expose serious security-related issues for users of the DNS. This report dives right into the technical discussion and is targeted at readers who have been following the issue. Those new to the issue should first read the introductory documents located at: http://www.icann.org/en/help/name-collision.

We 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. The modalities, risks, and etiologies of the inevitable DNS namespace collisions in new TLD namespaces will resemble the collisions that already occur routinely in the other parts of the DNS. The addition of multiple new TLDs over the past decade (generic and country code) has not suggested that new failure modalities might exist; rather, the indication is that the failure modalities are similar in all parts of the DNS namespace. Our research has shown that a very few root causes are responsible for nearly all collisions, and these root causes appear in nearly every classification of TLD, albeit in varying proportions.

That said, DNS namespace collisions are a complex and pervasive occurrence that manifests throughout the global Internet DNS namespace. Collisions in all TLDs and at all levels within the global Internet DNS namespace have the ability to expose potentially serious security and availability problems and deserve serious attention. While current efforts to expand the global DNS namespace have collision-related implications, the collision problem is bigger than new TLDs and must be viewed in this context.

In summary, our recommendations describe a comprehensive approach to reducing current and future DNS namespace collisions, alerting operators of potential DNS namespace related issues, and providing emergency response capabilities in the event that critical (e.g., life safety) systems are adversely impacted.

DNS namespace collisions exist outside of, and independently from, the current efforts to expand the DNS namespace. These collisions have almost certainly existed since the emergence of a global public DNS. As early as 2003, multiple researchers have pointed to the existence of queries into undelegated space received at the root.[1,2,3,4] Our research shows that every TLD that has been added to the root since

---

[1] *Understanding DNS Evolution*, Castro, Zhang, John, Wessels, claffy, 2010, http://www.caida.org/publications/papers/2010/understanding_dns_evolution/understanding_dns_evolution.pdf

[2] *Is Your Caching Resolver Polluting the Internet?*, Wessels, 2004, http://dns.measurement-factory.com/writings/wessels-netts2004-paper.pdf

[3] *RFC 4697: Observed DNS Resolution Misbehavior*, Larson, Barber, 2006, http://tools.ietf.org/html/rfc4697

consistent data collection has occurred (2007) has exhibited some symptoms of collision activity prior to delegation.

The issue of collisions is not specific to TLDs; rather, risk exists wherever a collision crosses an administrative control boundary in the DNS. Said differently, the most dangerous DNS namespace collisions occur when *the resulting DNS query is resolved by a different administrative party than expected by the querier*. This makes intuitive sense. Because of the hierarchical nature of the DNS, the vast majority of administrative control separations occur at the TLD and Second Level Domain (2LD) levels.

Over the course of the study, JAS found no evidence to suggest that the security and stability of the global Internet DNS itself is at risk. This finding confirms the results of the *DNS Stability String Review* performed on each string during Initial Evaluation pursuant to Section 2.2.1.3.1 of the Applicant Guidebook (AGB).[5,6] The remainder of our research is focused on issues from the perspective of end-systems as consumers of the global DNS.

When faced with a range of unknowns and hypotheticals, it is important not to overlook emergent facts and experience. As we write this update, 275 New gTLDs have been delegated and over 835,000 second level registrations have been added. TLDs representative of the complete range of the taxonomy JAS developed (see Section 3.4) are represented. .berlin – a geographic term that our research suggests is heavily present in DNS search paths – has the third largest number of registrations of all new TLDs. .email and .link – short, technology-oriented generic terms that our research suggests are present in a number of hardcoded configurations – rank 6th and 7th respectively, each with over 30,000 2LD registrations. .company, .solutions, and .agency – terms that our research suggests are commonly hardcoded into small business-oriented configurations – are also delegated and have thousands of registrations each. Neither JAS nor ICANN is aware of even a single instance of a problematic collision. Of course, this fact certainly doesn't "prove the negative" but it also can't be ignored at this point.

Certainly the nature of the string impacts the drivers behind colliding behavior. As we presented at Verisign's *Workshop and Prize on Root Causes and Mitigation of*

---

[4] *Wow, that's a lot of packets,* Wessels, Fomenkov, 2003, http://www.caida.org/publications/papers/2003/dnspackets/wessels-pam2003.pdf

[5] *gTLD Applicant Guidebook*, ICANN, 2012, http://newgtlds.icann.org/en/applicants/agb

[6] The process followed by ICANN's vendor for this review, Interisle Consulting Group, process is documented at http://newgtlds.icann.org/en/program-status/evaluation-panels/dns-stability-process-07jun13-en.pdf

Name Collisions (WPNC)[7] in London, strings with the potential to introduce new failure etiologies have been introduced into the TLD in the past. .post (delegated in 2012) saw the most collision activity prior to delegation of any of the nine TLDs added since 2007. .post is interesting because "post" is also an HTTP method and a not insignificant proportion of the collisions appeared to be related to erroneous DNS lookups of text intended to be transmitted to an HTTP server. History provides lessons and data regarding the introduction of a variety of strings at the TLD.

We believe the introduction of new TLDs offers an opportunity to educate operators regarding DNS namespace collisions and help find and remedy potential collision-related issues that may be present in their systems. As such, we recommend implementation of a 90-day "controlled interruption" period for all approved new TLDs with the exception of .corp, .home, and .mail. Registries that have not yet been delegated to the root zone shall implement controlled interruption via wildcard records; registries that have elected the "alternative path to delegation" shall implement controlled interruption by adding appropriate resource records for the labels appearing in their respective block lists. Following the 90-day controlled interruption period, registries will not be subject to further collision-related restrictions. Like the Certificate Authority (CA) revocation approach, which may be partially implemented in parallel, we believe the 90-day controlled interruption period offers a conservative buffer between potential legacy usage of a TLD and the new usage.

Lacking clear RFC 1918-like guidance directing operators to DNS namespaces safe for internal use, several such namespaces have been "appropriated" for this purpose over the years. While the etiology is subtly different, the .corp and .home TLDs are clear outliers in this respect; the use of .corp and .home for internal namespaces/networks is so overwhelming that the inertia created by such a large "installed base" and prevalent use is not likely reversible. We also note that RFC 6762 suggests that .corp and .home are safe for use on internal networks.[8]

Given that the Internet has demonstrated a need for RFC 1918-like DNS namespaces, we recommend that .corp and .home be referred to the Internet Engineering Task Force (IETF) for potential RFC 1918-like protection/treatment. [9]

---

[7] http://namecollisions.net

[8] *RFC 6762: Multicast DNS* (appendix G), Cheshire, Krochmal, 2013, http://tools.ietf.org/html/rfc6762

[9] RFC 6761 may be the appropriate vehicle for implementing a permanent reservation.

Like .corp and .home, the TLD .mail also exhibits prevalent, widespread use at a level materially greater than all other applied-for TLDs. Our research found that .mail has been hardcoded into a number of installations, provided in a number of example configuration scripts/defaults, and has a large global "installed base" that is likely to have significant inertia comparable to .corp and .home. As such, we believe .mail's prevalent internal use is also likely irreversible and recommend reservation similar to .corp and .home and similarly recommend ICANN not delegate that TLD at this time.

RECOMMENDATION 1: The TLDs .corp, .home, and .mail be referred to the Internet Engineering Task Force (IETF) for potential RFC 1918-like protection/treatment.

JAS uncovered a vulnerability not directly related to ICANN's New gTLD Program nor to new TLDs in general that has the potential to impact end-systems. Pursuant to ICANN's Coordinated Vulnerability Disclosure Process,[10] ICANN shall: "...privately disclose information relating to a discovered vulnerability to a product vendor or service provider ("affected party") and allow the affected party time to investigate the claim, and identify and test a remedy or recourse before coordinating the release of a public disclosure of the vulnerability with the reporter." Furthermore, ICANN's process states: "All parties to the disclosure generally agree to refrain from disclosing the vulnerability to the public until a remedy is identified and tested or until the threat is considered contained."

After extensive discussions with impacted vendors and ICANN executives, JAS is concerned that publication of the experimental methods and data contained in the complete JAS report may accelerate discovery of the vulnerability and/or serve to facilitate exploitation of the vulnerability after it is discovered. As such, pursuant to ICANN's process and out of an abundance of caution, JAS has recommended against publication of a complete report at this time.

A description of our expected Phase Two report appears in a section 3.4; the Phase Two report will be published as soon as it is prudent.

[10] *Coordinated Vulnerability Disclosure Reporting at ICANN*, ICANN, 2013, https://www.icann.org/en/about/staff/security/vulnerability-disclosure-05aug13-en.pdf

2.1 Summary of Recommendations

RECOMMENDATION 1: The TLDs .corp, .home, and .mail be referred to the Internet Engineering Task Force (IETF) for potential RFC 1918-like protection/treatment.

RECOMMENDATION 2: ICANN continue efforts to make technical information available in fora frequented by system operators (e.g., network operations groups, system administration-related conferences, etc.) regarding the introduction of new gTLDs and the issues surrounding DNS namespace collisions.

RECOMMENDATION 3: Emergency response options are limited to situations where there is a reasonable belief that the DNS namespace collision presents a clear and present danger to human life.

RECOMMENDATION 4: Root-level de-delegation of a production TLD is not considered as an emergency response mechanism under any circumstances.

RECOMMENDATION 5: ICANN leverage the EBERO mechanisms and functionality to respond to DNS namespace-related issues. ICANN must have the following capabilities on a 24x7x365, emergency basis: 1). Analyze a specific report/incident to confirm a reasonable clear and present danger to human life; 2). Direct the registry on an emergency basis to alter, revert, or suspend the problematic registrations as required by the specific situation; 3). Ensure that the registry complies in a timely manner; and 4). Evaluate and monitor the specific situation for additional required actions. Furthermore, we recommend that ICANN develop policies and procedures for emergency transition to an EBERO provider in the event the registry is unable and/or unwilling to comply. We recommend ICANN maintain this capability indefinitely.

RECOMMENDATION 6: ICANN require new TLD registries to publish the controlled interruption zone immediately upon delegation in the root zone. After the 90-day period, there shall be no further collision-related restrictions on the registry.

RECOMMENDATION 7: ICANN require registries that have elected the "alternative path to delegation" rather than a wildcard, instead 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 90 days. After the 90-day period, there shall be no further collision-related restrictions on the registry.

RECOMMENDATION 8: ICANN relieve the prohibition on wildcard records during the controlled interruption period.

RECOMMENDATION 9: ICANN monitor the implementation of controlled interruption by each registry to ensure proper implementation and compliance.

RECOMMENDATION 10: ICANN work with the IETF to identify a mechanism for IPv6 that provides similar functionality to that available in IPv4's "localhost" reserved prefix.

RECOMMENDATION 11: ICANN, DNS-OARC, and the root operators explore a medium-latency, aggregated summary feed describing queries reaching the DNS root.

RECOMMENDATION 12: ICANN, DNS-OARC, and the root operators explore establishment of a single, authoritative, and publicly available archive for historical data related to the root.

RECOMMENDATION 13: ICANN explore collecting NXDOMAIN entries in DNS query logs from registry operators and contribute them to an independent data repository such as DNS-OARC for further analysis. To limit the potential for commercial gaming or use by malicious parties, we recommend that logs be provided six months in arrears.

RECOMMENDATION 14: ICANN request that the appropriate bodies further explore issues relating to collisions in existing DNS namespace, the practice of "domain drop catching," and the associated data feeds that may be leveraged by attackers when attempting to exploit collisions.

2.2 Acknowledgements

JAS is grateful for the constructive engagement by numerous members of the community. We specifically want to recognize and thank:

- the Security and Stability Advisory Committee (SSAC) for thoughtful and valuable interaction while we drafted this report;
- Burt Kaliski and his team at Verisign Labs, for extensive and insightful public comments, valuable interaction with the JAS team throughout our study, and for their overall leadership on this issue including hosting the *Workshop and Prize on Root Causes and Mitigation of Name Collisions* (WPNC) in London;
- Farsight Security for contributing valuable data;
- OpenRegistry for contributing valuable data; and
- our longtime partner simMachines for their analytical contributions.

3 Detection and Response

Since risk cannot be totally eliminated, a comprehensive approach to risk management contains some level of *a priori* risk mitigation combined with investment in detection and response capabilities. Consider fire protection; most major cities have *a priori* protection in the form of building codes, detection in the form of smoke/fire alarms, and response in the form of 9-1-1, sprinklers, and the fire department.

In terms of detecting problematic DNS namespace collisions, the initial symptoms will almost certainly appear through various IT support mechanisms, namely corporate IT departments and the support channels offered by hardware/software/service vendors and Internet Service Providers. When presented with a new and non-obvious problem, professional and non-professional IT practitioners alike frequently turn to Internet search engines for answers. This suggests that a good detection/response investment would be to "seed" support vendors/fora with information/documentation about this issue in advance and in a way that will surface via search engines when IT folks begin troubleshooting. We collectively refer to such documentation as "self-help" information. ICANN has already begun developing documentation designed to assist IT support professionals with namespace-related issues.[11]

RECOMMENDATION 2: ICANN continue efforts to make technical information available in fora frequented by system operators (e.g., network operations groups, system administration-related conferences, etc.) regarding the introduction of new gTLDs and the issues surrounding DNS namespace collisions.

One valuable suggestion from Google in the public comment period[12] is to stagger introduction of the Controlled Interruption periods such that impacted parties have a reprieve between the detection and mitigation phases of their response. However, staggered Controlled Interruption periods will have the side effect of causing intermittent failures, which are maddening and hard to diagnose from a system administrator perspective. Moreover, we found that systems configured in a way to create collision-related effects in the existing DNS namespaces routinely experience and tolerate intermittent failures (for example, when using a different DNS resolver) so intermittent failures are likely to resemble the status quo for impacted systems, and not communicate a problem. We believe a sustained and consistent Controlled Interruption period is the best opportunity to communicate with administrators.

---

[11] *Name Collision Resources & Information*, ICANN, retrieved January 2014, http://www.icann.org/en/help/name-collision

[12] http://forum.icann.org/lists/comments-name-collision-26feb14/pdfBGWsaf8Vuk.pdf

However, providing advice to system administrators regarding technical mechanisms they may deploy to temporarily gain reprieve during Controlled Interruption is valuable. Such advice may include the use of Response Policy Zones to temporarily rewrite query responses to something non-problematic (presumably NXDOMAIN), temporarily becoming authoritative for certain zones, etc. We recommend ICANN augment the existing technical advice to system administrators with such temporary remediation information and techniques.

It is likely that in the vast majority of expected cases, the IT professional "detectors" will also be the "responders" and any issues detected will be resolved without involving other parties.[13] However, situations in which other parties may be expected to have a role in response must be considered.

For the sake of this discussion, assume that an Internet user is experiencing a problem related to a DNS namespace collision. The term "Internet user" is intended broadly as any application, system, or device that is a consumer of the global Internet DNS. At this point in the thought experiment, disregard the severity of the problem. The affected party (or parties) will likely exercise the full range of typical IT support options available to them – vendors, professional support, IT-savvy friends and family, and Internet search. If any of these support avenues are aware of ICANN, they may choose to contact ICANN at some point. Let's further assume the affected party is unable and/or unwilling to correct the technical problem themselves and ICANN is contacted – directly or indirectly.

There is a critical fork in the road here: Is the expectation that ICANN will provide technical "self-help" information or that ICANN will go further and "do something" to technically remedy the issue for the user? We consider the options below in an escalating progression:

Option 1: ICANN provides technical support above and beyond "self-help" information to the impacted parties directly, including the provision of services/experts. Stated differently, ICANN becomes an extension of the impacted party's IT support structure and provides customized/specific troubleshooting and assistance. *We rule out this option as inappropriate and out-of-scope for ICANN.*

Option 2: At ICANN's request, referral, or direction, the registry provides technical support above and beyond "self-help" information to the impacted parties directly, including the provision of services/experts. Stated differently, the registry becomes an extension of the impacted party's IT support structure and provides customized/specific troubleshooting and assistance. *We rule out this option as inappropriate and out-of-scope for a registry.*

[13] Availability issues are typically detected internally whereas security issues are often detected by third parties and reported to the system operators.

Option 3: ICANN forwards the issue to the registry with a specific request to remedy. In this option, assuming all attempts to provide "self-help" are not successful, ICANN would request that the registry make changes to their zone to technically remedy the issue. This could include temporary or permanent removal of second level names and/or other technical measures that constitute a "registry-level rollback" to a "last known good" configuration. *We consider this option feasible but undesirable as it creates considerable opportunity for operational complexities and unintended consequences. This option should only to be used in excessively serious circumstances.*

Option 4: ICANN initiates a "root-level rollback" procedure to revert the state of the root zone to a "last known good" configuration, thus (presumably) de-delegating the impacted TLD. In this case, ICANN would attempt – on an emergency basis – to revert the root zone to a state that is not causing harm to the impacted party/parties. *We consider this option feasible but even more undesirable as it creates considerable opportunity for operational complexities and unintended consequences. This option should only to be used in excessively serious circumstances after all previous mitigation attempts have failed.*

We note that ICANN's New gTLD Collision Occurrence Management Plan and SAC062 contemplate some of these emergency response options in a broad sense.

In any theater of operations – not just the global Internet DNS – emergency responders must be mindful of "cure is worse than the disease" scenarios wherein the response actually creates additional risks, harms, and significant potential for unintended consequences. Because of the potential operational impacts to the global Internet DNS, changes to the root zone are not to be taken lightly.

From a practical perspective, we conclude that the de-delegation of a TLD in the root would effectively be a permanent death for that TLD regardless of whether the TLD reappeared in the future.[14] This is a steep price for a registry to pay for anything but the most egregious and flagrant disregard for a serious harm.

Obviously, the severity of the harm is a critical variable. In risk analysis, severity is almost always measured economically and from multiple points of view. Any party expected to "do something" will be forced to choose between two or more economically motivated actors: users, registrants, registrars, and/or registries experiencing harm. We must also consider that just as there may be users negatively impacted by new DNS behavior, there may also be users that are

[14] While we note that there has always been some degree of churn in the root zone, the commercial pressures on the current new gTLDs significantly elevate the impact of a de-delegation, no matter how short.

dependent upon on the new DNS behavior. Unfortunately, we cannot give equal consideration to actors that are following the technical standards vs. those depending on technical happenstance or poorly implemented software for proper functionality.

Even attempting to weigh economic harm or "national security" on a global basis creates a slippery slope and forces registries and ICANN to arbitrate impossible scenarios. Concepts like "national security," "law and order," and "key economic processes" do not translate well on a global basis and risk another "Morality and Public Order" debate – which is exactly what happened when similar terms were introduced into the ICANN landscape previously. Unfortunately, there will not be time for such a debate in real-time, leaving emergency responders forced to make rapid decisions concerning extremely serious issues – like root-level changes – in a non-deterministic state.

Moreover, an emergency response threshold that is not well defined risks weaponization of the mechanism by commercial or government interests. Sadly, recent history has shown some governments will use a full range of tools to silence distribution of certain viewpoints over Internet channels. It is also reasonable to assume that commercial interests will attempt to "game" any mechanism for competitive advantage.

As such, we recommend that emergency response be limited to scenarios where there is a reasonable belief that the DNS namespace collision presents a clear and present danger to human life. While admittedly a high bar, we believe it is the only deterministic and non-debatable option. We feel creating a path to emergency response (including root-level changes) based on lesser factors is unwise.

Despite the previous recommendation, ICANN must prepare for the worst-case scenario. Fortunately, ICANN has already developed an emergency response mechanism as a part of the Emergency Back-End Registry Operator (EBERO) Program. The EBERO Program is designed to quickly respond to a variety of registry-level technical SLA failures; response options include an emergency (and potentially involuntary) transition of an entire registry to a new operator using a robust process that is highly scripted and exercised.

We recommend that, if necessary (in the event of an unresponsive or non-cooperative registry), a "root-level rollback" be implemented via EBERO as opposed to simply removing a TLD from the root. Shifting a registry to EBERO and making subsequent surgical changes is a superior approach to wholesale removal of an entire production TLD – including potentially many 2LD registrations that are not causing harm.

RECOMMENDATION 3: Emergency response options are limited to situations where there is a reasonable belief that the DNS namespace collision presents a clear and present danger to human life.

RECOMMENDATION 4: Root-level de-delegation of a production TLD is not considered as an emergency response mechanism under any circumstances.

In the case of severe harm being exposed by a DNS namespace collision where the registry is unable or unwilling to take action (by altering or suspending a second level registration), ICANN could transfer the registry to an EBERO on an emergency basis and instruct the EBERO to make the required second level change to remedy the harm. While we recognize any "root-level rollback" is highly undesirable, ICANN should maintain the capability, thus ensuring that timely action can be taken in all circumstances.

RECOMMENDATION 5: ICANN leverage the EBERO mechanisms and functionality to respond to DNS namespace-related issues. ICANN must have the following capabilities on a 24x7x365, emergency basis: 1). Analyze a specific report/incident to confirm a reasonable clear and present danger to human life; 2). Direct the registry on an emergency basis to alter, revert, or suspend the problematic registrations as required by the specific situation; 3). Ensure that the registry complies in a timely manner; and 4). Evaluate and monitor the specific situation for additional required actions. Furthermore, we recommend that ICANN develop policies and procedures for emergency transition to an EBERO provider in the event the registry is unable and/or unwilling to comply. We recommend ICANN maintain this capability indefinitely.

3.1 Approach to Delegation

The delegation of new TLDs presents a unique opportunity to raise awareness of the DNS namespace collision issue and help system operators identify and mitigate potential issues. Therefore, we recommend a "controlled interruption" approach as described below. The idea for controlled interruption springs from past DNS-related experiences and is conceptually similar to a "trial delegation" as proposed in SAC062.

3.1.1 Controlled Interruption

The infamous Microsoft Hotmail domain expiration in 1999[15] and other similar domain expirations led to the implementation of ICANN's Expired Registration Recovery Policy.

More recently, Regions Bank made news[16] when their domains expired, and undoubtedly countless other similar events go unreported. In the case of Regions Bank, the Expired Registration Recovery Policy seemed to work exactly as intended – the interruption inspired immediate action and the problem was solved, resulting in only a bit of embarrassment. Importantly, there was no opportunity for malicious activity.

For the most part, the Expired Registration Recovery Policy is effective at preventing unintended expirations due to the application of "controlled interruption." The Expired Registration Recovery Policy calls for extensive notification before the expiration, then a period when "the existing DNS resolution path specified by the Registrant at Expiration ("RAE") must be interrupted" – as a last-ditch effort to inspire the registrant to take action.

Nothing inspires urgent action more effectively than service interruption.

But critically, in the case of the Expired Registration Recovery Policy, the interruption is immediately corrected if the registrant takes the required action – renewing the registration. It's nothing more than another notification mechanism – just a more aggressive round after all of the passive notifications failed. In the case of a registration in active use, the interruption will be recognized immediately, inspiring urgent action.

---

[15] *Good Samaritan squashes Hotmail lapse?*, Hansen/CNET, December 27, 1999, retrieved January 2014, http://news.cnet.com/2100-1023-234907.html

[16] *Regions Bank website down, domain not renewed?*, Walsh/al.com, April 15, 2013, retrieved January 2014, http://www.al.com/business/index.ssf/2013/04/regions_bank_website_down_doma.html

Like unintended expirations, DNS namespace collisions can be viewed as a notification problem. The system administrator utilizing the colliding namespace (either knowingly or unknowingly) must be notified and take action to preserve the security and stability of their systems.

Leveraging a controlled interruption to raise awareness of DNS namespace collisions draws on the effectiveness of the Expired Registration Recovery Policy with the implementation looking like a modified "Application and Service Testing and Notification (Type II)" trial delegation as proposed in SAC62. But instead of responding with pointers to application layer listeners (or "honeypots"), the authoritative nameserver responds with an address inside 127/8 – the range reserved for Loopback. We recommend this approach be applied to A queries directly and MX and SRV queries via an intermediary A record (the vast majority of collision behavior observed in DITL data stems from A and MX queries).[17]

Responding with an address inside 127/8 will likely interrupt any application depending on an NXDOMAIN or some other response, but importantly also prevents traffic from leaving the requestor's host and does not facilitate a malicious actor's ability to intercede. In the same way as the Expired Registration Recovery Policy calls for "the existing DNS resolution path specified by the RAE [to] be interrupted", responding with a localhost reserved address should encourage immediate action by the requesting party while not exposing them to new malicious activity.

If legacy/unintended use of a DNS name is present, one could think of controlled interruption as a "buffer" or "cooling-off" period prior to use by a legitimate new registrant. This is similar to the CA Revocation Period as proposed in the New gTLD Collision Occurrence Management Plan that "buffers" the legacy use of certificates in internal namespaces from new use in the global DNS. As we discussed at ICANN Singapore, and Verisign's *Workshop and Prize on Root Causes and Mitigation of Name Collisions* (WPNC) in London, 30 to 90 day buffer periods are also commonly deployed in other large important namespaces like postal and phone numbering systems to provide feedback when changes occur. Like the CA Revocation Period approach, a set period of controlled interruption is deterministic for all parties. Unfortunately, human nature often requires a hard deadline to inspire urgent action.

Moreover, instead of using the typical 127.0.0.1 address for localhost, we recommend using a unique "flag" IPv4 address: 127.0.53.53. Because the primary objective is to communicate with system administrators through their logs, this unique and strange IP should stand out in log files, be noticed, and result in the administrator searching the Internet for assistance (we note that as of today, using Google to search for "127.0.53.53," the top 5 results are relevant). Making it known

[17] AAAA query load suggests that collisions related to IPv6 space are far less pervasive.

that new TLDs will behave in this fashion and publicizing the flag IP (along with self-help materials) will help administrators isolate the problem more quickly than just using the common 127.0.0.1. As hosts often have listening sockets bound to 127.0.0.1, this approach also reduces the probability of creating issues related to those servers. We also suggest that system administrators proactively search their logs for this flag IP address as a possible indicator of problems. Enterprise-wide sensors in the form of DNS query log analysis or Network Intrusion Detection Systems (NIDS) such as SNORT provide an enterprise perspective.

Numerous experiments performed by JAS confirmed that a wide range of application layer software logs something resembling a "failed connection attempt to 127.0.53.53" which is the desired behavior. We also confirmed that all modern Microsoft, Linux, Apple, and BSD-derived operating systems correctly implement RFC 1122 (albeit with variations[18]) and keep the traffic within the host system, not transmitted over the network. This includes Linux and Windows-derived embedded operating systems. Of particular importance is Windows XP because our research has indicated that Windows XP is used extensively in industrial control and other embedded systems.

Additionally, we encourage ICANN and the IETF to work with software vendors eventually incorporate functionality and tools to notice DNS queries that respond with this flag IP address and provide meaningful assistance. One could imagine a meaningful event in the Windows Event Log describing the situation if a DNS query returns the flag IP, browsers displaying helpful diagnostic information instead of simply stating "Connection Timeout," etc.

The ability to "schedule" the controlled interruption serves to further mitigate possible effects. One concern in dealing with collisions is the reality that a potentially harmful collision may not be identified until months or years after a TLD goes live – when a particular second level string is registered. A key advantage to applying controlled interruption to all second level strings in a given TLD in advance and at once via wildcard is that most failure modes will be identified during a scheduled time and before a registration takes place. This has many positive features, including easier troubleshooting and the ability to execute a far less intrusive rollback if a problem does occur. From a practical perspective, avoiding a complex string-by-string approach is also valuable.

The Expired Registration Recovery Policy mandates that the disruption may be for as few as eight days. However, our experiments indicate that the disruptions

[18] Some implementations route the entire /8 to localhost whereas other implementations use a host route resulting in only a /32 being dedicated to localhost. The resulting behavior during a connection attempt is slightly different, but indicative of failure in both cases.

associated with controlled interruption as proposed may be more subtle, justifying a longer disruption period.

We believe the 90-day CA Revocation Period is sufficiently conservative (recall, we characterized our initial recommendation – 120 days – as "exceedingly conservative"). Given the potential seriousness of DNS namespace collisions and the immense value of detecting a harmful collision prior to a registry entering General Availability (GA), we believe the conservative approach is also warranted and recommend a 90-day controlled interruption period.

If there were to be a catastrophic impact, a surgical reversal of a 2LD registration could be implemented relatively quickly, easily, and with low risk while the impacted parties worked on a long-term solution. A new registrant and associated new dependencies would likely not be adding complexity at this point. Our recommended 90-day controlled interruption period is an ample and conservative detection and cure period for impacted parties.

Implementation of controlled interruption achieves these objectives:

- Helps notify system administrators of possible improper use of the global DNS;
- Protects these systems from malicious actors during a cure period;
- Doesn't direct potentially sensitive traffic to registries, registrars, Internet hosts/honeypots, or other third parties;
- Inspires urgent remediation action;
- Is low risk with limited opportunity for unintended consequences; and
- Is easy to implement and deterministic for all parties.

We therefore recommend controlled interruption be implemented by each new TLD registry by publishing a zone similar to the following:

```
$ORIGIN TLD
$TTL 1H
@      IN     MX 10 your-dns-needs-immediate-attention
*      IN     MX 10 your-dns-needs-immediate-attention
@      IN     SRV 10 10 0 your-dns-needs-immediate-attention
*      IN     SRV 10 10 0 your-dns-needs-immediate-attention
@      IN     TXT "Your DNS configuration needs immediate attention see URL"
*      IN     TXT "Your DNS configuration needs immediate attention see URL"
@      IN     A 127.0.53.53
*      IN     A 127.0.53.53
```

We note that some versions of popular DNS servers (notably BIND[19]) do not properly validate DNSSEC signed query responses to wildcards in all cases.

[19] *Bug 390 - NSD does not return closest provable encloser NSEC3 on wildcard queries*, NLnet Labs, May 26, 2011, retrieved January 2014, https://www.nlnetlabs.nl/bugs-script/show_bug.cgi?id=390; also note ISC RT ticket #26200

However, we also note the potential difficulties and confusion that could arise when treating the controlled interruption zones differently than production zones from an operational perspective. We have considered the tradeoffs and recommend that registries DNSSEC sign the controlled interruption zone using the same policies and procedures they intend to use when the zone is in production. A client downstream of a flawed DNS server may in some situations be "interrupted" due to the DNS server's inability to validate the signature as opposed to an interruption due directly to controlled interruption.

We recommend that the registry implement the controlled interruption period immediately upon delegation in the root zone and the prohibition on wildcard records be temporarily suspended during this period. Given the objective of controlled interruption and the reality that no registrant data will be in the zone at this point, we believe that temporarily permitting wildcard records for this purpose is not counter to established ICANN prohibitions on wildcard records and does not raise the concerns that lead ICANN to establish these prohibitions. [20]

RECOMMENDATION 6: ICANN require new TLD registries to publish the controlled interruption zone immediately upon delegation in the root zone. After the 90-day period, there shall be no further collision-related restrictions on the registry.

However, implementing a wildcard record is not prudent for a registry in GA. As such, we recommend publishing A and SRV resource records for labels in the ICANN 2LD Block List for the 90-day controlled interruption period. While arguably not an exhaustive list of queries, the 2LD block lists as currently constructed provide an adequate inventory[21,22] of queries sent by long-lived systems, which are the ones of most concern. The alternative – wildcard records in production zones – is less attractive and counter to established ICANN prohibitions.[23]

---

[20] *SSAC Report: Redirection in the com and net Domains,* ICANN Security and Stability Advisory Committee (SSAC), July 9, 2004, retrieved January 2014, http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf

[21] *Public Comments on Proposal to Mitigate Name Collision Risks by Google Inc.*, Google Inc., September 17, 2013, retrieved January 2014, http://forum.icann.org/lists/comments-name-collision-05aug13/pdfkwCAlijJOp.pdf

[22] *Is Your Caching Resolver Polluting the Internet?*, Wessels, 2004, http://dns.measurement-factory.com/writings/wessels-netts2004-paper.pdf

[23] *SSAC Report: Redirection in the com and net Domains*

With the exception of .corp, .home, and .mail, this approach would apply to all registries, including the registries not eligible for the "alternative path to delegation." ICANN will make 2LD Block Lists available as required.

RECOMMENDATION 7: ICANN require registries that have elected the "alternative path to delegation," rather than a wildcard, instead 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 90 days. After the 90-day period, there shall be no further collision-related restrictions on the registry.

RECOMMENDATION 8: ICANN relieve the prohibition on wildcard records during the controlled interruption period.

RECOMMENDATION 9: ICANN monitor the implementation of controlled interruption by each registry to ensure proper implementation and compliance.

3.1.2 Why 90 days?

By far the most prevalent public comments to our draft report were related to the 120-day Controlled Interruption period. We reviewed these comments carefully and subsequently modified our thinking.

A portion of the public comment from .Club Domains, LLC sums up the issue nicely:

> *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.*[24]

We like this comment because it speaks to the trade-offs between potential risks/harms and actual risks/harms. In New TLD space, Controlled Interruption is a conservative mitigation against a theoretical harm. Despite a concentrated effort by a number of researchers (JAS included!) for the better part of the past two years to find actual incidences of collision-induced harms related to New TLDs, the reality is that none have been found. As of today, 275 New gTLDs have been delegated and over 835,000 2LD registrations have been added with no indication of issues. As we stated earlier, while this certainly doesn't "prove the negative," the data must be taken into consideration. Based on everything we know now, the harms remain theoretical. Given no indication of actual harms, is it justifiable for JAS to recommend an "excessively conservative" and atypical duration, or is a "merely conservative" and more typical duration more appropriate? What is the tradeoff – what *actual* harms could we be causing with an "excessively conservative" approach to a theoretical harm?

After reviewing this issue, we have changed our recommendation to indicate a 90-day Controlled Interruption period.

[24] http://forum.icann.org/lists/comments-name-collision-26feb14/pdfEVFexxB8GK.pdf

3.1.3 What about IPv6?

Since IPv6 does not support a range of addresses for localhost like IPv4, there is not a straightforward analog of our Controlled Interruption recommendation in v6 space. So the discussion becomes twofold: (1) is a v6 response necessary, and if so, (2) what address would be returned?

Addressing the first, we do not believe v6 responses are necessary at this time. The data we analyzed revealed a miniscule number of resolvers seeking v6-only responses (less than 1%) where the resolver doesn't appear to be dual-stacked. As of this writing, Google reports that roughly 3.5% of their users access Google over v6.[25] So while v6 adoption is certainly important and growing, v6-only hosts experiencing a DNS namespace collision does not appear to be a real problem today.

Regarding the second item, an address that is not a direct conceptual equivalent to 127.0.53.53 in v4 space would need to be selected (or "appropriated") for the purpose of Controlled Interruption. While experts can certainly debate this topic (we considered ::1, ::53, IP addresses within fd00::/8, fe80::/10, and ::ffff:127.0.53.53) at the end of the day each approach has plusses, minuses, and importantly the potential for unintended consequences. It's critical to remember that v6 implementations are comparatively young when compared to v4 implementations; the behavior of the vast majority of v4 stacks when presented 127.0.53.53 is well understood whereas the behavior of v6 implementations and their associated infrastructure when presented with ::53, fd00::53, or ::ffff:127.0.53.53 is certainly less deterministic.

So we're left with a tradeoff: do we risk potential unintended consequences of experimenting in the "fringes" of v6 for what is very likely a small benefit? Do we risk causing new problems to address what is fairly clearly a corner case? At the end of the day, we are left with no strong rationale for a v6 response and numerous reasons to be cautious of the potential for unintended consequences.

That being said, v6 support is certainly desirable in the long-term. One possible solution is working with the IETF to extend the definition of localhost to ::0/64 instead of ::1/128 to create a direct equivalent of the 127/8 space in IPv4. We recommend that ICANN work with the IETF to identify a workable long-term solution for IPv6.

[25] https://www.google.com/intl/en/ipv6/statistics.html

RECOMMENDATION 10: ICANN work with the IETF to identify a mechanism for IPv6 that provides similar functionality to that available in IPv4's "localhost" reserved prefix.

3.1.4 Controlled Interruption Trial

In January, JAS deployed the controlled interruption zone in multiple 2LD namespaces that exhibited evidence of significant collision and collision-like behavior.

As we had previously established bi-directional communication with multiple parties querying these names, we gave our contacts advance notice that we were making changes to the zone and asked them to observe and report the behavior of their systems during the controlled interruption windows.

Despite publishing phone numbers and email addresses via http and Whois, in the event the controlled interruption caused harm, not a single call or email was received. Additional details of this trial will be available in a future report.

3.1.5 Alternatives to Controlled Interruption

We considered several alternatives to controlled interruption as described above, including several honeypot approaches, use of DNAME, and various 2LD string-by-string and TLD-by-TLD approaches. While we eventually concluded that controlled interruption approach offers the most value and presents the least risk, discussion of alternatives is worthwhile.

3.1.6 String-by-String Approaches (TLD and 2LD)

While the occurrence and risk associated with DNS namespace collisions is not uniform across all TLDs and 2LDs, our analysis concluded that any collision and any harm could – at least in theory – occur anywhere in the global DNS namespace. We found ample evidence supporting this conclusion, and found that it would be a quixotic undertaking to determine the root cause of every incidence of a DNS namespace collision.[26] With the exception of .corp, .home, and .mail, which are clear outliers for the reasons mentioned earlier, the several root causes we found are not limited to particular strings, new or existing TLDs, or even specific levels of the DNS.

JAS' assessment is, with the exception of .corp, .home, and .mail, that the risk of a collision in the newly applied-for TLD namespaces causing more than a highly localized disruption is low after the recommended mitigation technique is applied. String-by-string and TLD-by-TLD approaches add significant complexity and

[26] *Focused Analysis on Applied-For gTLDs - .cba*, Verisign Inc., September 15, 2013, retrieved January 2014, http://forum.icann.org/lists/comments-name-collision-05aug13/msg00039.html

potential for unintended consequences while adding little if any security value. Not a good tradeoff. As such, we recommend an approach that addresses the root causes and does not delineate between specific strings unnecessarily.

3.1.7 Honeypot Approaches

Significant discussion has occurred in several fora regarding various implementations of a trial delegation that directs traffic to an Internet-based honeypot. The honeypot, run by ICANN or some trusted third party, could serve two functions: 1) Present helpful information for operators reaching the site over http and potentially other protocols; and 2) Collect logs to help identify volume, sources, and potential severity of collision and collision-like activity. Some ideas describe a honeypot that runs for a deterministic time period while others continue the honeypot until some threshold is achieved indicating risk has been mitigated to an (undefined) acceptable level.

Because collisions are largely a notification problem, we like the concept of honeypot approaches. However, there are some critical traits of honeypot approaches that make them undesirable.

- Whenever logs are collected, the question "for what purpose" must be asked. How much collision activity is "OK" – what is the acceptable risk? Is the threshold the same for all TLDs? Are all query sources to be treated equally – that is, do we look differently upon log entries that *appear* to be from a nuclear power plant vs. a residential broadband network? These questions, being subjective in nature, may not have answers that can achieve consensus.
- Whenever logs are collected, we must also be vigilant for gaming opportunities. Because there are many interested parties and significant commercial pressures, we assume that competing interests will attempt to exploit any activity that may create an argument for slowing or halting valuable registrations in a TLD. Even the possibility (perceived or actual) of such gaming will virtually assure that gaming occurs.
- There are collision scenarios where returning an Internet IP address will cause traffic to be sent over the Internet that was never previously sent. Ever conscious of "cure being worse than the disease" concerns, we certainly do not want to open these hosts to new risks while we try to help them. Additionally, we are informed by the vulnerability we discovered on this matter; for machines impacted by the issue, honeypotting a popular port will *assure* that sensitive information is transmitted in the clear over the LAN and the Internet to the honeypot. Absent the honeypot, transmission of this sensitive information is not assured. Controlled interruption should not *decrease* the security posture of a system, even temporarily. Or, as Verisign cleverly said in their public comment,

we don't want to risk turning "Controlled Interruption" into "Controlled Exfiltration!"[27]

- As security researchers have long known, a lot of potentially sensitive information appears in logs. Usernames and passwords regularly appear in http logs. Other protocols raise similar concerns. Our experience confirms that any advertised honeypot IP will receive a host of sensitive information. Managing this information – and convincing the global Internet community that the data is being handled responsibly – is another hurdle with any honeypot approach.
- Different global legal jurisdictions place restrictions on data collected after it was "solicited." As advertising a honeypot IP could be argued as "soliciting traffic," the resulting data may have legal protections, further adding to the complexity.
- Very limited experience exists related to large-scale honeypotting of the service discovery protocols and corporate directory protocols that dominate colliding DNS queries. SAC06[28] contains a lengthy discussion of the unintended consequences of these sorts of interactions with non-HTTP protocols. There is sufficient risk of causing collateral damage and unintended consequences.

The final four bullets describe our rationale for a 127/8 IP address that does not cause traffic to leave the host, thereby avoiding those pitfalls.

We also considered a variation wherein the honeypot would be an RFC 1918 IP address as opposed to an Internet address – thereby allowing private network operators to monitor and capture the resulting traffic. However, we ruled out this variation due to the potential for unintended consequences if the RFC 1918 IP happened to be in use in the network where the affected party resides, and because of the potential for causing general confusion. An operator with the requisite sophistication to redirect or capture RFC 1918 traffic likely also has the requisite sophistication to react appropriately to 127/8 responses.

[27] http://forum.icann.org/lists/comments-name-collision-26feb14/pdffjLkIlhcj4.pdf
[28] https://www.icann.org/en/system/files/files/report-redirection-com-net-09jul04-en.pdf

3.1.8 DNAME Approaches

We considered multiple schemes using DNAME records in an attempt to emulate similar controlled interruption behavior. While we eventually concluded that these schemes are not feasible and less effective than localhost-based ideas, discussion is worthwhile.

One option could be implemented via DNAME records in the root. We quickly considered this option infeasible due to the difficulties, unknowns, and potential for unintended consequences surrounding the placement of DNAME records in the root; furthermore, such an approach is very likely not compatible with the IANA/Verisign/NTIA root zone management system as currently implemented and may require modifications to the IANA Functions contract.

However, using wildcards in the delegated zone is a more viable option and emulates most of the desired behavior.

Consider a wildcard DNAME record within the origin of the TLD zone pointing to some identifiable target (e.g., "you-need-to-change-your-dns-config-see-collisions-dot-icann-dot-org."). The target should not be resolvable in order to force an NXDOMAIN response (note that this assumes the specific DNAME implementation returns an NXDOMAIN instead of SERVFAIL or something else – given the relative newness of DNAME in the DNS protocol suite and its lack of significant exercise in implementations, unusual implementation decisions and/or behavior can't be ruled out).

When considering DNAME approaches, client support is a paramount concern. While the experiments[29] conducted by Geoff Huston and George Michaelson are valuable and informative, they are biased to heavy clients and human browsing (running Flash and receiving ads). The situation before us is far less biased to these types of clients, so client support is in question at best. Proper support of DNAME (RFC 2672 circa 2000) in legacy, possibly misconfigured, devices is probably less likely than proper localhost support (RFC 1122 circa 1989).

DNAME-based approaches do offer additional flexibility when compared to localhost redirection approaches, specifically in the ability of sophisticated operators to observe, control, and redirect the responses. But again, an IT operation sophisticated enough to control DNAME queries certainly has plenty of other options available to manage DNS namespace collisions. Catering to sophisticated IT

[29] *draft-jabley-dnsop-as112-dname-01: AS112 Redirection using DNAME*, Abley, Dickson, Kumari, Michaelson, October 12, 2013, retrieved January 2014, http://tools.ietf.org/html/draft-jabley-dnsop-as112-dname-01 (see *Appendix A: Assessing Support for DNAME in the Real World*)

operators by providing flexibility and options seems to come at the expense of simplicity, predictability, and widespread client support.

Finally, DNAME-based approaches don't necessarily interrupt, negating the whole purpose of controlled interruption. The DNAME redirect to return NXDOMAIN means folks can continue on as they're currently doing. They won't notice anything so they won't fix it, defeating the purpose of the interruption.

As such, we consider DNAME-based approaches inferior to localhost-based approaches.

3.2 Root Level Data, Monitoring, and Day-In-The-Life (DITL)

We blogged[30] about our experiences using the DNS-OARC-maintained "DITL" datasets; these datasets are truly invaluable albeit limited for researchers looking into global Internet DNS traffic. Conscious of the calls for additional datasets and monitoring at the root level, we want to discuss the objectives of monitoring and logging systems at a meta level.

When considering monitoring and logging systems, one must always start with the "for what purpose" questions. Different data consumers have different requirements. For example, operators interested in emergency response demand a low-latency, actionable, "ticket" type of monitoring. They want the "this hard drive is dead" ticket as soon as possible after it dies. Capacity planners want intermediate-latency data with some ad hoc aggregation and trending capabilities to answer questions like "how much data do we have and what is the growth rate?" Product managers want high-latency, highly detailed data repositories that can answer a full range of complex ad hoc queries to observe behaviors, trial new product ideas, etc.

Obviously, these very different consumers have very different requirements driving very different technical implementations.

We observe that from an availability standpoint, low-latency ticket/availability data is already available for the root. Albeit in a highly decentralized fashion, the DNS root is probably one of the most highly monitored systems on Earth in that regard.

Conversely, DITL datasets are at the other end of the spectrum: extremely high latency (one 50 hour period annually), voluminous and unstructured data suitable only for compute-intensive ad hoc analysis by expert researchers.

While individual root operators certainly have a full range of data available to them, there is nothing in the middle available to researchers or the Internet at large.

Looking from a slightly different angle, the *availability* and *content* of the root is exceptionally well monitored with low latency but the *queries* to the root are much less visible.

We believe there is a need for a medium-latency, aggregated, and more "consumable" data stream from the root operators containing aggregated summary data describing the queries seen by the root. This new feed should be in a reasonably accessible and well-documented format like CSV, XML, or YAML and

---

[30] *Demystifying DITL Data [Guest Post]*, Kevin White, JAS Global Advisors LLC, November 16, 2013, retrieved December 2013, http://domainincite.com/15068-demystifying-ditl-data-guest-post

ideally have latency on the order of a few days. Mindful of the numerous issues surrounding such an undertaking, we recommend that ICANN, DNS-OARC, and the root operators explore such a mechanism.

We note ongoing efforts by the Root Server System Advisory Committee ("RSSAC") to address monitoring, and the forthcoming publication of RSSAC 002: *Recommendations on Measurements of the Root Server System.* We applaud the proactive efforts of some root operators to increase the fidelity of root server monitoring.

RECOMMENDATION 11: ICANN, DNS-OARC, and the root operators explore a medium-latency, aggregated summary feed describing queries reaching the DNS root.

Over the course of our research, we were also surprised to find that authoritative historical information regarding the contents of the root zone is not always available. A significant proportion of historical information is only captured informally in email threads and in the heads of various luminaries. As such, we also recommend that a single, authoritative archive for root data be established.

RECOMMENDATION 12: ICANN, DNS-OARC, and the root operators explore establishment of a single, authoritative, and publicly available archive for historical data related to the root.

We recognize that data and measurement regarding the DNS namespace collision phenomenon is important. One of the attractive features of a honeypot approach is a new, high fidelity, and low latency data stream describing this behavior. In lieu of the honeypot, we recommend ICANN explore collecting NXDOMAIN and Controlled Interruption (127.0.53.53 query response) entries in DNS query logs from registry operators and contribute them to an independent data repository such as DNS-OARC where they may be analyzed by the research community. To limit the potential for commercial gaming or use by malicious parties, we recommend that logs be provided six months in arrears. If such logs are collected commencing with delegation, the long-term effectiveness of Controlled Interruption may be measured; we believe it important to be informed by these metrics when considering future mitigation techniques in delegated and un-delegated DNS namespace.

RECOMMENDATION 13: ICANN explore collecting NXDOMAIN and Controlled Interruption (127.0.53.53 query response) entries in DNS query logs from registry operators and contribute them to an independent data repository such as DNS-OARC for further analysis. To limit the potential for commercial gaming or use by malicious parties, we recommend that logs be provided six months in arrears.

3.3 Collisions in Existing DNS Namespace

Because of the popularity of .com, typical software behavior, and common DNS search path configurations/practices, collisions at the 2LD level within .com likely occur at a higher frequency than collisions at any other location in the DNS (2LD and TLD). Because of the sheer size and prevalence of .com, this is not unexpected. With respect to collisions, .com is victim of its own success. Recently, other researchers have quantified the order of magnitude of collisions within .com using different datasets.[31] Noted security researcher Robert Stucke spoke at DEFCON 21 about vulnerabilities he discovered by leveraging DNS namespace collisions within .com.[32]

Researching collisions in existing TLD namespaces was a part of our engagement. Over the course of this study, JAS registered several 2LDs to enhance our understanding of this phenomenon and collect additional data. Based on behaviors uncovered during our research, we made educated guesses as to where problematic collisions may occur. These registrations immediately generated a surprising amount of traffic.

It is worth noting that while selecting 2LDs to register for our research, we made use of publically available tools designed to facilitate "domain drop catching" and various "squatting" activities. One such tool offers to the public the ability to find 2LDs within .com that are "available with traffic" – the very definition of a DNS namespace collision – at the second level within the Internet's most popular TLD.

While we understand the commercial value of this service, as security practitioners we are deeply concerned about this type of functionality. As such, we recommend that ICANN request that the appropriate bodies (GNSO, SSAC, etc.) further explore issues relating to collisions in existing DNS namespace, the practice of "domain drop catching," and the associated data feeds that may be leveraged by attackers when attempting to exploit collisions.

RECOMMENDATION 14: ICANN request that the appropriate bodies further explore issues relating to collisions in existing DNS namespace, the practice of "domain drop catching," and the associated data feeds that may be leveraged by attackers when attempting to exploit collisions.

[31] http://forum.icann.org/lists/comments-name-collision-05aug13/pdf056yDnxGje.pdf

[32] http://www.youtube.com/watch?v=ZPbyDSvGasw

3.4 Description of Forthcoming Phase Two Report

JAS uncovered a vulnerability not directly related to ICANN's New gTLD Program nor to new TLDs in general that has the potential to impact end-systems. In fact, the vulnerability manifested while researching collisions within .com while analyzing collisions in existing TLDs (please see below). Pursuant to ICANN's Coordinated Vulnerability Disclosure Process,[33] ICANN shall: "...privately disclose information relating to a discovered vulnerability to a product vendor or service provider ("affected party") and allow the affected party time to investigate the claim, and identify and test a remedy or recourse before coordinating the release of a public disclosure of the vulnerability with the reporter." Furthermore, ICANN's process states: "All parties to the disclosure generally agree to refrain from disclosing the vulnerability to the public until a remedy is identified and tested or until the threat is considered contained." As such, pursuant to ICANN's process and out of an abundance of caution, JAS has recommended against publication of a complete report at this time.

The Phase Two report is expected to contain the following information:

Impact of malware/adware/clickfraud tools: We found that malware, adware, and clickfraud tools generated a significant proportion of the random and pseudo-random string queries. We also identified other potential sources of algorithmic queries. In the Phase Two report, we will describe this occurrence and provide specific details and supporting data. It is worth noting that we previously discussed this finding in presentations in ICANN Buenos Aires, ICANN Singapore, and Verisign's *Workshop and Prize on Root Causes and Mitigation of Name Collisions* (WPNC) in London.[34] Queries related to malware/adware/clickfraud tools explain in excess of 20% of the colliding queries revealed in DITL datasets.

Analysis of Collisions in previous TLD delegations: We found that collisions have occurred prior to delegation of every TLD since (at least) 2007 and presented high-level data to this effect at the WPNC in London and ICANN Singapore. Said differently, collisions in the DNS namespace are certainly not a new phenomenon (please also see Section 2 above). In the Phase Two report, we will further describe this occurrence and provide specific details and supporting data.

Analysis of Collisions in existing TLDs: As stated in Section 3.3 above, JAS is very concerned about collisions in existing DNS namespace and the tools that facilitate discovery of colliding names. In the Phase Two report, we will describe these

[33] *Coordinated Vulnerability Disclosure Reporting at ICANN*, ICANN, 2013, https://www.icann.org/en/about/staff/security/vulnerability-disclosure-05aug13-en.pdf

[34] http://namecollisions.net

phenomena, including the methods we used to discover the vulnerabilities, locate vulnerable hosts, and datasets where appropriate.

A Taxonomy of Queries and TLDs: We classified behavior leading to collisions and created a high-level description of each applied-for TLD based on the colliding queries present in DITL datasets. Organizing the classification into a taxonomy leads to an understanding that: (1) a very few root causes seem to explain the vast majority of colliding behavior, and (2) nearly all root causes appear in all TLDs in differing proportions. Only .corp, .home, and .mail are clear outliers.

The classification was based on: (1) the diversity of querying source IP addresses and Autonomous Systems; (2) the diversity of labels queried; (3) applying sophisticated "randomness detection" to strings and substrings; (4) presence of linguistic terms and colloquialisms in strings and substrings; (5) temporal patterns; and (6) analysis of the Regular Expressions of the labels queried within each TLD and across all TLDs. Aside from improving our understanding of the behavior within .corp, .home, and .mail, we eventually found that the taxonomy does not directly translate to mitigation techniques. Mitigation techniques addressing the small number of root causes are applicable to all TLDs. Dr. Arnoldo Muller-Molina, Founder and Chief Data Scientist of our partner simMachines presented some information about the classification research we performed at the closed DNS-OARC workshop in Warsaw, Poland in May 2014.[35] We also note that the JAS public comment submission included an analysis of colliding queries over a few of the aforementioned dimensions.[36]

Sources, methods, and experimental results: Over the course of this study, we performed a number of experiments and collected a significant amount of data. We talked to a number of vendors, consultants, and end-users experiencing collisions in existing namespaces today. We purchased a number of names and collected data. Several sources contributed data. The types of analysis we performed have been alluded to in this paper and in our presentations at ICANN Singapore, the WPNC in London, and the DNS-OARC workshop in Warsaw. Phase Two of this report will contain the full detail of these activities and relevant datasets.

[35] https://indico.dns-oarc.net//contributionDisplay.py?sessionId=1&contribId=30&confId=19
[36] http://forum.icann.org/lists/comments-name-collision-05aug13/pdf3WmZlrH3fo.pdf

SAC066
SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions

A Comment from the ICANN
Security and Stability Advisory Committee (SSAC)
6 June 2014

Preface

This is a Comment to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning the JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions. The SSAC advises the ICANN community and Board on matters relating to the security, stability, and integrity of the Internet's naming and address allocation systems. This includes operational matters (*e.g.*, pertaining to the correct and reliable operation of the root name system), administrative matters (*e.g.*, pertaining to address allocation and Internet number assignment), and registration matters (*e.g.*, pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Comment, references to SSAC members' biographies and statements of interest, and SSAC members' dissents to or withdrawals from the findings or recommendations in this Comment are at the end of this Comment.

Table of Contents

Executive Summary

The Security and Stability Advisory Committee (SSAC) has reviewed the Report prepared for ICANN by JAS Global Advisors (herein referred to as the "JAS") entitled "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report." It has identified eight issues, and makes recommendations in relation to each of them. A summary of the recommendations is provided below; context, motivation, and discussion are provided in the sections that follow. The recommendations fall into two categories: those related to operational considerations and those related to strategic considerations.

Operational Recommendations:

- The Internet Corporation for Assigned Names and Numbers (ICANN) should expand the range of situations that would trigger an emergency response, for example national security, emergency preparedness, critical infrastructure, key economic processes, commerce, and the preservation of law and order.

- Instead of a single controlled interruption period, ICANN should introduce rolling interruption periods, broken by periods of normal operation, to allow affected end-user systems to continue to function during the 120-day test period with less risk of catastrophic business impact.

- ICANN should perform an evaluation of potential notification approaches against at least the requirements provided by the SSAC prior to implementing any notification approach.

- ICANN should implement a notification approach that accommodates Internet Protocol Version 6 (IPv6)-only hosts as well as IP Version 4 (IPv4)-only or dual-stack hosts.

- ICANN should provide clarity to registries on the rules and the method of allocation of blocked names after the conclusion of the test period.

Strategic Recommendations:

- ICANN should consider not taking any actions solely based on the JAS Phase One Report. If action is planned to be taken before the entire report is published, communications to the community should be provided to indicate this clearly.

- ICANN should in due course publish information about not yet disclosed issues.

- ICANN should seek to provide stronger justification for extrapolating findings based on one kind of measurement or data gathering to other situations.

1. Introduction

The term "name collision" refers to the situation where a name that is defined and used in one namespace may also appear in another. Users and applications intending to use a name in one namespace may actually use it in a different one, and unexpected behavior may result where the intended use of the name is not the same in both namespaces. The circumstances that lead to a name collision could be accidental or malicious. In the context of top level domains (TLDs), the conflicting namespaces are the global Internet Domain Name System (DNS) namespace reflected in the root zone as published by the Root Zone Management Partners (currently the Internet Corporation for Assigned Names and Numbers (ICANN), the U.S. Department of Commerce National Telecommunications and Information Administration (NTIA), and Verisign) and any other namespace, regardless of whether that other namespace is intended for use with the DNS or any other protocol.

With respect to collisions with names provisioned under ICANN's new generic TLD (gTLD) program, on 26 February 2014 ICANN published a report entitled "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report," prepared for ICANN by JAS Global Advisors (hereinafter referred to as the "JAS Phase One Report")[1]. The JAS Phase One Report provides a set of recommendations that support an approach for identifying and managing the impact of current and future DNS namespace collisions, notifying operators of potential DNS namespace related issues and providing emergency response capabilities in the event that critical systems related to human health and safety are adversely impacted.

The SSAC thanks ICANN and the JAS for their efforts in addressing the name collision issue and the opportunity to comment on this work. In particular, the SSAC appreciates the constructive cooperation and collaboration of ICANN and JAS in providing, on a number of occasions, further information and clarification to inform the production of this report.

[1] See "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report" at http://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-26feb14-en.pdf.

2. SSAC Comments

2.1 Clear and Present Danger to Human Life

a. Summary of JAS Recommendation

Recommendation 3 of the JAS Phase One Report states:

> "Emergency response options are limited to situations where there is a reasonable belief that the DNS namespace collision presents *a clear and present danger to human life*."

b. SSAC Comment

Recommendation 3 sets too high a barrier for the application of emergency response options. Limiting emergency response options to the situation of a "clear and present danger to human life" ignores a broad range of scenarios that may have substantial detrimental impact on, for example, national security, emergency preparedness, critical infrastructure, security protocols and mechanisms such as anti-virus software, key economic processes, commerce, or markets and the preservation of law and order.

c. SSAC Recommendation

Recommendation 1: ICANN should expand the range of situations that would trigger an emergency response, for example national security, emergency preparedness, critical infrastructure, key economic processes, commerce, and the preservation of law and order.

In making this recommendation, the SSAC recognizes that every situation will require the exercise of judgment and few decisions will be black and white.

2.2 Controlled Interruption Period

a. Summary of JAS Recommendation

Recommendation 6 of the JAS Phase One Report states:

> "ICANN require new TLD registries to publish the controlled interruption zone immediately upon delegation in the root zone. After the 120-day period, there shall be no further collision-related restrictions on the registry."

b. SSAC Comment

The JAS approach means that service for collision-affected users would be interrupted until those users are able to identify and fix the collision problem. This interruption could be as long as 120 days. A company that relied upon impacted systems to process payroll, track and order inventory, schedule customer visits, etc., might experience unreasonably lengthy business interruption.

It is also possible that only the most technically sophisticated system administrators will be aware of the potential for this type of service interruption and even fewer will be able to implement remediation easily, especially since no remediation techniques are currently offered to enable collision occurrence management.

While every approach to controlled interruption involves balancing trade-offs and exercising judgement, the SSAC considers that the single controlled interruption period as proposed in the JAS Phase One Report is not the optimal approach to test for, identify and remediate name collisions.

c. SSAC Recommendation

Recommendation 2: Instead of a single controlled interruption period, ICANN should introduce rolling interruption periods, broken by periods of normal operation, to allow affected end-user systems to continue to function during the 120-day test period with less risk of catastrophic business impact.

Controlled interruption periods starting at 24 hours and eventually lengthening to 30 days would be separated by periods of at least 3 days, to allow users or system administrators to identify or develop and put in place solutions or workarounds. Collisions detected during the earlier controlled interruption periods would potentially be resolved before the next interruption period. Even though the resolution periods will need to be long, recognizing that no resolution options are currently being considered as part of this occurrence management framework, this approach would at least eliminate prolonged downtimes and induced outages for end users and enterprises.

The rolling interruption periods should be lengthened as they progress to trigger collisions that occur at lower frequencies: e.g., only once every 7 days. For example, a process that may fail due to a collision might only be run weekly or monthly, and so a controlled interruption period of less than a week or month would not necessarily catch the collision. These longer interruption periods will also attract the attention of users or system administrators who may have ignored a shorter interruption period on the assumption that the (unknown) problem had been resolved.

Lastly, the controlled interruption does not have be a separate event in the overall launch sequence. It could run in parallel with some other periods,

2.3 Use of Localhost "Flag" IP Address

a. Summary of JAS Recommendation

The JAS Phase One Report recommends that during the test period the operator of the TLD use a unique "flag" IP address (127.0.53.53) to notify system administrators:

> "Because the primary objective is to communicate with system administrators through their logs, this unique and strange IP will hopefully be noticed and the administrator will search the Internet for assistance."

Use of this "Flag" address facilitates investigation by some end-user system administrators, but not for end-users in general.

b. SSAC Comment

The SSAC believes that the principal requirements for a notification system are:

1. *Effective Communication.* The chosen system should pass relevant information to affected parties effectively, via notification messaging and/or if possible, in a direct manner, recognizing that the target audience is a combination of technical system administrators and non-technical end-users. Examples of notification messaging could include Intrusion Defense System/Intrusion Prevention System/Data Leak Prevention (IDS/IPS/DLP) systems alerts, third party notifications from honeypot operators, or log file analysis. Direct notification could include application failures (non-resolution errors), walled-garden style web page notifications, and local log files. At minimum, "relevant information" should include the nature of the problem experienced by the user and a link to a page containing supplementary information including contact information for those responsible for administration of the test period (in case emergency response is requested) and the schedule for the test period.

2. *Measurability*. The chosen system should be measurable, such that it is possible to gauge the impact of name collisions and track how the impact changes with time. With a threshold of "Clear and Present Danger to Human Life" being designated, it is important to be able to determine when such a threshold could be reached. The SSAC's broader recommendations on threshold levels call for richer data collection. Measurements should at least include, but not be limited to, amount of traffic, types of traffic, and sources of traffic.

3. *Minimum Harm.* The chosen system should minimize the potential for collateral damage. For instance, address-based redirection has the potential to impact not only a huge array of standard protocols, but also non-standard protocols used within enterprises. The leakage of Personally Identifiable Information (PII) is an example of such collateral damage. External actors appointed to implement a

> mitigation system (e.g. appointed honeypot operators) must operate under a high standard of care.

Based on these three measures of effectiveness for a notification system, the SSAC would draw a different conclusion to the JAS Phase One Report on the most appropriate notification system. The JAS report seems to place privacy concerns ahead of other criteria such as effective notification and measurability and consequently recommends the "flag" address. However the SSAC considers that a wealth of operational experience exists in minimizing PII exposure by honeypots.

The SSAC advises ICANN to perform an evaluation against at least the criteria articulated above prior to implementing any notification approach. The SSAC has performed an initial analysis in Appendix A for community review. The SSAC understands that additional confidential information available to ICANN but not publicly released will most likely have an impact on the evaluation.

c. SSAC Recommendation

Recommendation 3: ICANN should perform an evaluation of potential notification approaches against at least the requirements provided by the SSAC prior to implementing any notification approach.

2.4 IPv4 Solution Only

a. Summary of JAS recommendation

Recommendation 7 of the JAS Phase One Report states:

> "ICANN require registries that have elected the "alternative path to delegation," rather than a wildcard, instead publish appropriate A and SRV resource records for the labels in the ICANN SLD Block List to the TLD's zone with the 127.0.53.53 address for a period of 120 days. After the 120-day period, there shall be no further collision-related restrictions on the registry."

b. SSAC Comment

The proposed approach of using the single "flag" address 127.0.53.53 for localhost is inadequate, as it is applicable to IPv4-only or dual-stack hosts only and does not support IPv6-only hosts. No direct equivalent exists in IPv6 space.

Support for IPv6-only clients is highly recommended. ICANN should deploy solutions with an eye to the future, and support for IPv6-only clients is necessary both to support the ongoing effort to deploy IPv6 on Internet-connected systems and to accommodate IPv6-only infrastructure that might be deployed internally, but for which dependencies on the global DNS namespace exist.

c. SSAC Recommendation

Recommendation 4: ICANN should implement a notification approach that accommodates IPv6-only hosts as well as IPv4-only or dual-stack hosts.

2.5 General Availability of Blocked Names

a. Summary of JAS recommendation

Recommendation 7 of the JAS Phase One Report states that:

> "ICANN require registries that have elected the "alternative path to delegation," rather than a wildcard, instead 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. After the 120-day period, there shall be no further collision-related restrictions on the registry."

b. SSAC Comment

ICANN has not specified any restrictions on the allocation and activation of blocked names after the conclusion of the test period. ICANN should consider providing clarity to registries on the rules and the method of allocation of these names (e.g. sunrise, Trademark Clearing House (TMCH), land rush, etc.).

c. SSAC Recommendation

Recommendation 5: ICANN should provide clarity to registries on the rules and the method of allocation of blocked names after the conclusion of the test period.

2.6 Name Collision Framework Not Complete

a. Summary of JAS Recommendation

The statement of work (SOW) developed by ICANN staff calls for the following deliverables[2] as part of a Name Collision Occurrence Management Framework:

1.1 Develop a Risk Assessment Model
  1.1.1 Impact of malware/adware/clickfraud tools
  1.1.2 Analysis of Collisions in previous TLD delegations
  1.1.3 Analysis of Collisions in existing TLDs

[2] "Statement of Work for the Development of the Name Collision Occurrence Management Framework", ICANN, November 11, 2013, https://www.icann.org/en/about/staff/security/ssr/name-collision-sow-11nov13-en.pdf.

1.1.4 Monte Carlo Analysis
1.1.5 Survey Instruments
1.1.6 Develop a Taxonomy of Queries
1.2 Options to manage risks

While not providing details of its analyses in the publicly released version of its Phase One report, JAS does recommend the following mitigation measures:

1. If the new gTLD is .CORP, .HOME, or .MAIL, then the entire new gTLD must be blocked indefinitely (indeed, "permanently")
2. If the new gTLD hasn't already been delegated, then the entire new gTLD must undergo a new process called "controlled interruption"
3. If the new gTLD has already been delegated, i.e., via the "alternate path" with an SLD block list[3], then the SLDs on the block list are subject to controlled interruption.

b. SSAC Comment

The SSAC acknowledges that the publicly released version of the JAS Phase One report is only intended to go part way to delivering the requirements of the SOW, and that the full detail of the Name Collision Occurrence Management Framework is work in progress. Noting that the SOW calls for the final Framework to incorporate comment and input from the ICANN Community, the SSAC looks forward to providing such comment when the full Framework, along with its associated analyses, is able to be made public.

c. SSAC Recommendation

Recommendation 6: ICANN should consider not taking any actions solely based on the JAS Phase One Report. If action is planned to be taken before the entire report is published, communications to the community should be provided to indicate this clearly.

2.7 Incomplete Report

a. Summary of JAS Recommendation

In the JAS Phase One Report, certain technical details, experimental methods, and data have been omitted until vulnerabilities discovered during the study have been remediated.

On page 3 the JAS Phase One Report states:

[3] See "New gTLD Security and Stability Considerations. Verisign Labs Technical Report #1130007", Version 2.2, March 28, 2013. http://www.verisigninc.com/assets/gtld-ssr-v2.1-final.pdf and "Reports for Alternate Path to Delegation Published", ICANN, November 17, 2013. http://newgtlds.icann.org/en/announcements-an6d-media/announcement-2-17nov13-en.

> "After extensive discussions with impacted vendors, JAS is concerned that publication of the experimental methods and data contained in the complete JAS report may accelerate discovery of the vulnerability and/or serve to facilitate exploitation of the vulnerability after it is discovered. As such, pursuant to ICANN's process and out of an abundance of caution, JAS has recommended against publication of a complete draft report at this time."

b. SSAC Comment

Without having visibility of all details of the background of the findings, it is hard for SSAC to give clear recommendations or to assess the validity of the findings. Thus the SSAC recommends that ICANN publish information about the vulnerabilities in due course, at which point the SSAC may further comment.

c. SSAC Recommendation

Recommendation 7: ICANN should in due course publish information about not yet disclosed issues.

2.8 The Nature of Collisions

a. Summary of JAS Recommendation

The JAS Phase One Report offers the assumption that:

> "The modalities, risks, and etiologies of the inevitable DNS namespace collisions in the new TLD namespaces will resemble the collisions that already occur routinely in other parts of the DNS."

b. SSAC Comment

Such an assumption would be fully justified if the types of names being introduced as new gTLDs were similar to those that have been introduced in the past. However, many of the new gTLDs are introducing commonly used words and place names which have a high probability of existing in already established domain names at the second and third levels, as well as existing in internal namespaces. This may give rise to other types of name collisions that did not arise in the course of previous delegations.

Thus, caution should be exercised in adopting any conclusions based on this assumption without extensive further study. Extrapolating findings based on one kind of data gathering to different scenarios should not be made without very detailed investigation of whether the extrapolation is justifiable, and what adjustments should be made to the findings. Testing and mitigation proposals should allow for the possibility that new types of name collisions will occur.

c. SSAC Recommendation

Recommendation 8: ICANN should seek to provide stronger justification for extrapolating findings based on one kind of measurement or data gathering to other situations.

3. Acknowledgements, Statements of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of all Committee members and any conflicts of interest—real, apparent, or potential—that may bear on the material in this document. The Dissents section provides a place for individual members to disagree with the content of this document or the process for preparing it. The Withdrawals section is a listing of individual members who have recused themselves from discussion of the topic. Except for members listed in the Objections and Withdrawals sections, this document has the consensus approval of all members of the Committee.

3.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this Comment.

SSAC Members:
Joe Abley
Don Blumenthal
Patrik Fältström
James M. Galvin
Julie Hammer
Warren Kumari
Danny McPherson
Ram Mohan
Rod Rasmussen
Mark Seiden

ICANN staff:
Julie Hedlund
Barbara Roseman
Steve Sheng (editor)

3.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/biographies-2014-06-06-en.

3.3 Dissents

There were no dissents to this Comment.

3.4 Withdrawals

David Conrad has withdrawn from this Comment due to a pre-existing relationship with JAS.

Appendix A: Alternative Notification Approaches

At a high level, there are at least four options for notifying potentially impacted parties, each occurring at varying stages in the transaction process. In this Appendix, the SSAC outlines these options, and provides an analysis.

1. **Do nothing.** Users of labels at any level of a domain name (e.g., www.corp.example.com, as a result of search lists [SAC064]), that collide with new gTLD strings in their operating environments will experience failures or misconnections and come to realize their configurations are problematic only after the new gTLD and domains within that gTLD are delegated and elicit operational impacts to their systems.

   SSAC Analysis: This approach provides no communication, is not measurable and does not attempt to mitigate any harm to any application or protocol. This is not acceptable, as previously conveyed by SSAC [SAC057 and SAC062]. Potentially impacted parties should be given some amount of forewarning and, ideally, context as well as an indication of potential remediation options. Vulnerabilities that result from name collisions may be subtle and might not necessarily result in immediately visible or distinctive failures.

2. Perform qualitative analysis of query sources as measured at root and TLD servers and provide proactive user notification.

   SSAC analysis: To perform qualitative analysis of query sources and notify users proactively, we need to have the ability to instrument measurements at the root server system or other levels of authoritative DNS, or to obtain the necessary visibility into other levels of the DNS hierarchy (e.g. recursive name server, end system, application, etc.) of recursion and caching in the system.[4] These temporal testing capabilities should be combined with a large-scale user education program.

   Given that we do not have these capabilities today, this approach is not a viable short-term option. Nevertheless, the SSAC notes that such measurement capabilities are needed, as previously recommended by SSAC in SAC045, SAC046, and SAC059. Such capabilities are also aligned with recommendations provided in SAC063 as it relates to DNSSEC Root Zone KSK Rollover.

3. Implement structured, short-term test periods ("controlled interruption"), in which end users utilizing a proposed gTLD will experience a failure, and then be given time (after each short-term test period) for planning and effectuating remediation efforts specific to their environment. This approach triggers the errors in a more controlled

[4] See Google Public Name Collision Comment, 2013, http://forum.icann.org/lists/comments-name-collision-05aug13/pdfkwCAlijJOp.pdf.

environment, and can be used as an early warning system to notify potentially impacted parties. There are two variations to notification in this approach:

3a: As recommended in the JAS Phase One Report, during the test period, the operator of the TLD will use a unique "flag" IP address (127.0.53.53) to notify system administrators.

SSAC Analysis: As a notification mechanism, the 127.0.53.53 approach requires system administrators noticing something unusual and then searching the Internet for assistance. It is unclear whether system administrators will notice or know what to do. Additionally, one of the main channels that system administrators will be notified of issues is through end-users. It is highly unlikely that end users will know what 127.0.53.53 might mean, let alone what to do with it.

The 127.0.53.53 approach does ensure no information leakage, and thus minimizes any privacy and legal issues from unintended connections. If minimizing information leakage is of the greatest concern, such an approach could be preferred.

3b: Instead of returning 127.0.53.53, addresses could be returned that direct the end user or system administrator to a web page that specifies the issue (a honeypot) and points to either potential solutions, or otherwise at least to Frequently Asked Questions (FAQs), documentation, consultants or expert groups who may be able to provide further information related the error condition and contextual remediation options. Care should be taken to cause minimal disruption to non-Hypertext Transfer Protocol (HTTP) requests directed at the honeypot.

SSAC analysis: As a notification mechanism, the honeypot offers the following advantages over 127/8:

- For HTTP traffic, the honeypot is more likely to get people's attention, and there is greater ability to disseminate information through a browser.
- For non-HTTP traffic, the honeypot is no worse a notification mechanism than the 127/8 approach.

As a data collection mechanism, honeypots could help operators and ICANN understand the scale of the impact of delegation by creating data streams that can be analyzed to understand the impact of a proposed TLD.

With the honeypot approach there is a risk of Personally Identifiable Information (PII) leakage. Traffic flow is created across the Internet and traffic is logged at the honeypot. Responses to non-HTTP transactions might introduce other collateral damage. If notification is a higher priority, then the honeypot approach could be preferred.

Extensive operational experience with such "honeypots" by various SSAC members (e.g., Internet Motion Sensor Project (IMS),[5] the Honeynet Project,[6] DNS changer[7]) suggests that this approach may be viable, and might lead to the best outcome, given the current impracticality of option 2 above, since it would provide the most direct mechanism for affected parties to be informed of such issues on their networks. The risk of exposure of PII or additional vulnerabilities to users could be managed with a clear data collection, retention and privacy policy. This approach would facilitate measurement of the impact of each controlled interruption and allow its effectiveness to be gauged. If we suppose such a honeypot only provided service over HTTP, and that inbound data from all other sources was refused in a manner designed to avoid client time-outs, the risk of collateral damage due to collection of data sent using non-HTTP protocols could be minimized.

[5] See Tracking Global Threats with the Internet Motion Sensor, NANOG 32, 2004. https://www.nanog.org/meetings/nanog32/presentations/bailey.pdf and The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets, USENIX SRUTI05, 2005,at https://www.usenix.org/legacy/event/sruti05/tech/full_papers/cooke/cooke_html/

[6] See at https://www.honeynet.org/.

[7] DNSchanger is the honeypot concept working at Internet scale. See: http://www.dcwg.org/.

Resources
- About ICANN
- Board
- Accountability & Transparency
- Governance
- Groups
- Contractual Compliance
- Registrars
- Registries
- ccTLDs
- Internationalized Domain Names
- TLD Acceptance

Approved Resolutions | Meeting of the New gTLD Program Committee

30 Jul 2014

1. Main Agenda

a. Name Collision Occurrence Management Framework

Whereas, on 7 October 2013 the NGPC directed the President, Global Domains Division to implement the proposal to manage the occurrence of collisions between new gTLDs and existing private uses of the same strings as presented in the "New gTLD Collision Occurrence Management Plan" (the "Collision Occurrence Management Plan"), and in doing so to take into account further advice that may be offered by Security and Stability Advisory Committee (SSAC)

and other experts and stakeholders.

Whereas, the Collision Occurrence Management Plan called for a follow-up study that would inform the development of a Name Collision Occurrence Management Framework.

Whereas, on 26 February 2014, ICANN published the follow-up study called for in the NGPC's 7 October 2013 resolution, which was prepared by JAS Global Advisors (JAS) and entitled "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report" [PDF, 322 KB] (the "JAS Study and Name Collision Framework"). The JAS Study and Name Collision Framework, which was posted for public comment, provided a set of recommendations that describe a comprehensive framework to reduce current and future DNS namespace collisions, alert operators of potential DNS namespace related issues, and provide emergency response capabilities in the event that critical (e.g., life safety) systems are adversely impacted. The JAS Study and Name Collision Framework was revised [PDF, 392 KB] in response to public comments.

Whereas, on 6 June 2014, the ICANN Security and Stability Advisory Committee (SSAC) published SAC 066 [PDF, 306 KB]: SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions, in which it offered advice and recommendations to the Board on the framework presented in the JAS Study and Name Collision Framework.

Whereas, the proposed name collision framework being presented to the NGPC for consideration takes into account advice offered by SSAC in SAC066, and the advice of other experts and stakeholders, including the recommendations from JAS, public comments, and community discussions at ICANN

meetings.

Whereas, the NGPC acknowledges comments from the community concerning the need to ensure that all names, which registries blocked under their Alternate Path to Delegation Report, be subject to the rights protection mechanisms established by the New gTLD Program.

Whereas, the ICANN Board previously adopted the NGPC's recommendation to direct the ICANN President and CEO to develop a long-term plan to management name collision at the root.

Whereas, the NGPC is undertaking this action pursuant to the authority granted to it by the Board on 10 April 2012, to exercise the ICANN Board's authority for any and all issues that may arise relating to the New gTLD Program.

Resolved (2014.07.30.NG01), the NGPC adopts the Name Collision Occurrence Management Framework <https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf> [PDF, 634 KB] to continue to manage the occurrence of collisions between new gTLDs and existing private uses of the same strings, and directs the President and CEO, or his designee(s), to take the necessary actions to implement the Name Collision Occurrence Management Framework. As part of implementation, registry operators will be provided with a Name Collision Occurrence Assessment (see Registry Agreement, Specification 6, Section 6), which will address, among other things, procedures to remove second level domains from the block list including measures to protect rights holders.

Resolved (2014.07.30.NG02), the NGPC directs the President and CEO, or his designee(s), to consult with the community during the next 90 days from the publication of these resolutions to address appropriate rights protection mechanisms for names

included in a registry operator's Alternate Path to Delegation Report and recorded in the Trademark Clearinghouse that registry operator withheld from allocation during its Sunrise period or Claims period.

Resolved (2014.07.30.NG03), the NGPC directs the President and CEO, or his designee(s) to provide information to, and work with the GNSO to consider whether policy work on developing a long-term plan to manage gTLD name collision issues should be undertaken.

Resolved (2014.07.30.NG04), the NGPC directs the President and CEO, or his designee(s), to continue to provide briefings and share information and best practices with ccTLD managers concerning name collision issues in light of the Name Collision Occurrence Management Framework.

Rationale for Resolution 2014.07.30.NG01 – 2014.07.30.NG04

Why is the NGPC considering this issue now?

The NGPC's action today follows on from its previous actions taken to address name collision issues. Specifically, on 7 October 2013, the NGPC took action directing the President, Global Domains Division to implement the proposal to manage the occurrence of collisions between new gTLDs and existing private uses of the same strings as presented in the "New gTLD Collision Occurrence Management Plan" (the "Collision Occurrence Management Plan"), and in doing so to take into account further advice that may be offered by Security and Stability Advisory Committee (SSAC) and other experts and stakeholders. A core feature of the Collision Occurrence Management Plan required ICANN to undertake additional study to develop a name collision occurrence management framework. The framework was intended to specify a set of collision occurrence assessments and corresponding

mitigation measures if any, that ICANN or new gTLD applicants may need to implement.

To implement the NGPC's 7 October 2013 action, on 24 February 2014, ICANN published a study prepared by JAS Global Advisors ("JAS") entitled "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report" (the "JAS Study and Name Collision Framework"). The JAS Study and Name Collision Framework provided a set of recommendations that describe a comprehensive framework to reduce current and future DNS namespace collisions, alerting operators of potential DNS namespace related issues, and providing emergency response capabilities in the event that critical (e.g., life safety) systems are adversely impacted. Additionally, the SSAC offered advice and recommendations to the Board on the proposed name collision framework included in the JAS Report in SAC 066: SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions [PDF, 306 KB].

At this time, the NGPC is adopting the Name Collision Occurrence Management Framework dated 30 July 2014 <https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf> [PDF, 634 KB], which is a final version of the framework called for in the Collision Occurrence Management Plan (the "Final Name Collision Framework"). The Final Name Collision Framework builds off of the framework in the JAS Study and Name Collision Framework, and has been further refined in response to the recommendations in SAC066, public comments, and additional community feedback during the ICANN Meeting in London. Adoption and implementation of the Final Name Collision Framework will allow ICANN to continue to move forward with the delegation of new gTLDs in a secure and stable manner.

What are the proposals being considered?

The Final Name Collision Framework being adopted by the NGPC presents a plan to manage the collision occurrences between new gTLDs and existing private uses of the same strings. A summary of some of the key elements of the Final Name Collision Framework is as follows:

General Requirements for Registries:

- Required to act on name collision reports from ICANN within two hours of the report during the first two years of the life of the TLD measured from the time of delegation of the TLD.

- Required to implement "controlled interruption" as the notification measure to alert parties that they may be leaking queries intended from private namespaces to the public DNS. Controlled interruption is required to be continuous interruption (i.e. not intermittent), and lasting for a 90-day period. Generally, if a TLD was delegated prior to a defined cut-off date, the registry operator would implement controlled interruption using MX, SRV, TXT, and A records for second level domains included in the block list. For TLDs delegated after a defined cut-off date, the registry operator would implement controlled interruption using a wildcard method. Controlled interruption (for IPv4) will use a loopback address (127.0.53.53)

Requirements for ICANN:

- Work within the IETF and with other relevant technical communities to identify a notification mechanism for IPv6 that provides similar functionality to that available in IPv4's "Loopback" reserved prefix.

- Defer delegating .MAIL indefinitely, and collaborate with the technical and security community to identify the best way to handle .MAIL (e.g. permanent reservation through the IETF process). The JAS Study and Name Collision Framework identifies .MAIL as exhibiting "prevalent, widespread use at a level materially greater than all other applied-for TLDs" and thus its prevalent internal use is likely irreversible.

- Produce new outreach and informational materials as needed to alert potentially affected parties about name collisions, and link to existing information regarding name collisions developed as part of the initial outreach campaign.

The NGPC's action today also addresses concerns raised by community regarding the need to ensure that names, which registries blocked under their Alternate Path to Delegation Report, be subject to applicable rights protection mechanisms established by the New gTLD Program. To address this concern, the NGPC is directing the President and CEO, or his designee(s), to consult with the community during the next 90 days (from the publication of these resolutions) to address appropriate rights protection mechanisms for names included in a registry operator's Alternate Path to Delegation Report and recorded in the Trademark Clearinghouse that registry operator withheld from allocation during its Sunrise period or Claims period.

To follow-up on a prior recommendation to the Board to direct the President and CEO to develop a long-term plan to management name collision at the root, the NGPC's action today directs the President and CEO, or his designee(s) to provide information to, and work with the GNSO to consider whether policy work on developing a long-term plan to manage gTLD name collision issues should be undertaken. The

NGPC also is taking action to direct the President and CEO, or his designee(s), to continue to provide briefings and share information and best practices with ccTLD managers concerning name collision issues in light of the adoption of the Final Name Collision Framework.

What Stakeholders or others were consulted?

ICANN initiated a public comment forum from 26 February to 21 April 2014, inviting the community to provide feedback on the JAS Study and Name Collision Framework. During the public comment period, twenty-eight comments were received. The public comment report summarizing the comments, and the full comments can be found at: https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf [PDF, 230 KB].

The SSAC also was consulted and offered advice and recommendations to the Board (via SAC066) on the proposed name collision framework included in the JAS Study and Name Collision Framework. Additionally, ICANN presented a version of the proposed Final Name Collision Framework during the ICANN Meeting in London.

What concerns or issues were raised by the community?

The JAS Study and Name Collision Framework received twenty-eight comments during the public comment period which were submitted by a full range of sources, including New gTLD applicants and those affiliated with applicants, corporations not directly affiliated with applicants, individual technology experts, and various DNS related industry organizations. Members of the community also submitted correspondence to ICANN regarding the intersection of name collision issues and rights protection mechanisms. Additionally, the SSAC raised

some concerns in SAC066 regarding the name collision framework.

Some key themes and concerns expressed by the SSAC and ICANN community included, but are not limited to the following:

- Concerns related to the current use of the Second Level Domain (SLD) Block Lists and the Alternate Path to Delegation in general.

- Concerns that the proposed 120-day "controlled interruption" period is too long and/or not justified – Some commenters suggested that there is no data to support having a 120-day controlled interruption period, and suggested that if there is a period, it should fall in the range of 45 days to 90 days.

- Concerns for using a "loopback" approach instead of a "honeypot" approach – The SSAC recommended that using a honeypot approach allows better notification for HTTP cases, and provides support for IPv4 and IPv6. Some of the public comments also suggest that a honeypot approach would provide a better opportunity to inform users of impending problems. Some other commenters, however, note that a honeypot may expose personally identifiable or sensitive information outside of the local network or to potential attackers, among other issues.

- Concerns about whether the controlled interruption should be continuous or intermittent – The SSAC recommended that instead of a single controlled interruption period, ICANN should introduce rolling interruption periods, broken by periods of normal operation, to allow affected end-user systems to continue to function during the test period with less risk of catastrophic business impact.

- Concerns about what type of event would trigger an emergency response – The SSAC recommended that ICANN should expand the range of situations that would trigger an emergency response, for example national security, emergency preparedness, critical infrastructure, key economic processes, commerce, and the preservation of law and order. Some of the public comments also raised concern that a "clear a present danger to human life" standard draws an arbitrary line, and others suggest that certain significant dangers to the business and financial sectors of the global economy might also merit the use of emergency measures.

- Concerns about the treatment of .CORP, .HOME, and .MAIL – Some of the public comments support the treatment of .CORP, .HOME, and .MAIL recommending in the JAS Study and Name Collision Framework, while others suggest that a final decision on this matter 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.

- Comments requesting the acceleration and closure of the collisions issue in general - Some members of the community noted a general concern that the name collision matter is being dealt with at such a late stage of the New gTLD process, and questioned why ICANN did not address the matter sooner. Commenters raising concerns about timing also requested that ICANN take action on the matter with deliberate speed so as not to cause further delay.

- Comments expressing concern about the interaction between the name collision block lists and intellectual property rights protection mechanisms – Some public comments and

correspondence to ICANN suggest that all names, which registries blocked 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), or other similar mechanism to protect rights holders. Additionally, some .BRAND TLD applicants note many of the "brand" terms included in the block lists are trademarks for the brand's products and services, and are seemingly generated at the root by the brand itself. These commenters suggest that ICANN consider an alternative process for .BRAND TLD applicants to expedite the release of such trademarked terms for their immediate use.

What significant materials did NGPC review?

The NGPC reviewed several materials, including, but not limited to the following:

- SAC057: The SSAC Report on Internal Name Certificates [PDF, 1.14 MB]
- SAC062: SSAC Advisory Concerning the Mitigation of Name Collision Risk [PDF, 382 KB]
- Name Collision in the DNS [PDF, 3.34 MB] – prepared by Interisle Consulting Group
- New gTLD Collision Occurrence Management Plan [PDF, 840 KB]
- Mitigating the Risk of DNS Namespace Collisions – A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report [PDF, 392 KB] (Final)
- Report of public comments on the JAS Study

and Name Collision Framework [PDF, 230 KB]

- SAC066: SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions [PDF, 306 KB]

What factors did the NGPC find to be significant?

The NGPC considered several significant factors during its deliberations over whether or not to adopt the Final Name Collision Framework. The following are among the factors the NGPC found to be significant:

- The NGPC considered the recommendations of the SSAC, including those in SAC066.

- As previously noted, several commenters, including the SSAC, raised concerns about using a "loopback" approach instead of a "honeypot" approach. In choosing the loopback approach in the Final Name Collision Framework, the NGPC took into consideration the privacy and legal risks associated with the honeypot approach described in SAC 062 and 066 and the JAS report. On balance, the NGPC notes that the notification features offered by using the loopback approach provides a better option to provide a notification system of name collisions while minimizing the issues inherent in using a honeypot approach. The NGPC also notes that while the honeypot approach has the benefit of offering a IPv6 solution, the Final Name Collision Framework includes a requirement that ICANN will work within the IETF and with other relevant technical communities to identify a mechanism for IPv6 that provides similar functionality to that available in IPv4's "Loopback" reserved prefix.

- The NGPC also found to be significant comments concerning whether the controlled interruption should be continuous or intermittent.

While the SSAC recommended an intermittent controlled interruption, it also acknowledged that every approach to controlled interruption involves balancing trade-offs and exercising judgment. From an operational perspective the intermittent approach presents more risk for registries and ICANN to implement and ensure correct functioning. On the other hand, continuous controlled interruption presents a more simple approach operationally and provides for an easier way to diagnose and troubleshoot. It also provides a more effective way to indicate the need for changes in an affected party's network configuration. Additionally, an intermittent controlled interruption approach in theory would allow an affected party to have temporary relief while the controlled interruption is in the "off" cycle. It should be noted that there is already a mechanism in place (name collision reporting) for affected parties to find temporary relief from name collision harm, if needed, making the intermittent approach an unnecessary burden.

- The NGPC considered the concerns raised by the community regarding the need to ensure that names, which registries blocked under their Alternate Path to Delegation Report, be subject to the rights protection mechanisms established by the New gTLD Program. As previously noted, to address these concerns, the NGPC is directing the President and CEO, or his designee(s), to consult with the community during the next 90 days (from the publication of these resolutions) to address appropriate rights protection mechanisms for names included in a registry operator's Alternate Path to Delegation Report and recorded in the Trademark Clearinghouse that registry operator withheld from allocation during its Sunrise period or Claims period.

- The NGPC considered the recommendations about what type of event would trigger an emergency response. The Final Name Collision Framework being adopted today will limit emergency response for name collision reports to situations where there is a reasonable belief that the name collision presents a clear and present danger to human life. The NGPC acknowledges SSAC advice with respect to expanding the range of situations that would trigger an emergency response. However, the NGPC notes that the severity of this risk (as in other cases) can be measured from multiple points of view; necessarily, there will be a decision between various impacted parties (i.e., the party that was using the domain name before it was delegated in the public DNS and the party that registered the name). Commercial interests could attempt to "game" a broader mechanism for competitive advantage. Concepts like "national security," "law and order", and "key economic processes" are not easily agreeable on a global basis. On the other hand, focusing on danger to human life is a more objective standard.

  Additionally, the Final Name Collision Framework includes an emergency response measure to address the unlikely case that a newly delegated gTLD creates a clear and present danger to human life as a result of colliding use as a dotless name. In this case, ICANN would work with the registry operator and ICANN's root zone management partners to reverse the new delegation. This would only happen during the 90-day wildcarded controlled interruption, during which there would be no names active (except "nic") under the TLD. Once the harm is mitigated, the gTLD registry operator may request again delegation. As indicated by SAC062 and the JAS Study and

Name Collision Framework report, reversal of a new delegation is an extreme measure and should be exercised in an extreme circumstance where there is clear and present danger to human life during the wildcarded controlled interruption period.

Are there Positive or Negative Community Impacts? Are there fiscal impacts/ramifications on ICANN (Strategic Plan, Operating Plan, Budget); the community; and/or the public? Are there any Security, Stability or Resiliency issues relating to the DNS?

SAC057 and the Name Collision Study identified several security risks to the DNS. The Final Name Collision Framework, as revised in response to community comments, and recommendations of the SSAC in SAC066 provides a path forward to delegating new gTLDs in a secure and stable manner.

The Final Name Collision Framework may have a fiscal impact on ICANN, the community or the public, as there may be additional costs associated with implementing the measures in the Final Name Collision Framework, including additional resources needed to continue the outreach campaign targeted to affected parties to help them identify and manage the name collision occurrences in their networks.

As part of ICANN's organizational administrative function, ICANN posted for public the name collision framework as presented in the JAS Study. The report of public comments is available at: https://www.icann.org/en/system/files/files/report-comments-name-collision-10jun14-en.pdf [PDF, 230 KB].

Published on 1 August 2014

Implementing Rights Protection Mechanisms in the Name Collision Mitigation Framework

1. Comment Phase
Ends 15 Sep 2014 23:59 UTC

2. Reply Phase
Ends 7 Oct 2014 23:59 UTC

3. Summary and Review

Follow Updates

Evaluation and Decision
During this phase your comments are reviewed by the body that asked for input/feedback and evaluations are made about how to proceed based on the comments.

Contents

Brief Overview

To determine the requirements on the appropriate Rights Protection Mechanisms for names removed from registry SLD Block Lists.

Comment Period: 25 Aug 2014 - 15 Sep 2014 23:59 UTC
Reply Period: 16 Sep 2014 - 7 Oct 2014 23:59 UTC

Section I: Description, Explanation, and Purpose

Consistent with the Name Collision Occurrence Management Framework [PDF, 926 KB] approved on 30 July 2014, the Board New gTLD Program Committee directed staff to provide each registry operator a Name Collision Occurrence Assessment ("Name Collision Assessment"), issued on 4 August 2014. Per the Name Collision Occurrence Assessment, for names included on the SLD Block List of the registry's Alternate Path to Delegation Report and recorded in the Trademark Clearinghouse that the registry withheld from allocation during its Sunrise Period or Claims Period, the registry must continue to withhold these names from allocation while ICANN consults with the community. This paper [PDF, 114 KB] examines operational and other considerations for several approaches regarding the appropriate Rights Protection Mechanisms for release of SLD Block List names.

Section II: Background

The Name Collision Assessment requires certain measures to be implemented for each top-level domain. In particular, it provides that for gTLDs delegated prior to 18 August 2014 who have activated names, the registry must ensure that second-level domain names desired to be activated from its SLD Block List after the 90-day controlled interruption period have been subject to applicable Rights Protection Mechanisms as required under Specification 7 of the Registry Agreement.

Based on feedback and discussion to date in the community regarding appropriate Rights Protection Mechanisms for names in the SLD Block list, several possible approaches are described in this paper for the handling of these names. ICANN is requesting community feedback on these alternatives, or proposals for additional measures.

Currently, names released from the SLD Block List after a TLD's Sunrise period has occurred are subject to the Trademark Claims service on release. Various stakeholder groups have provided feedback suggesting alternatives, for

example, a required Sunrise period, or a similar period incorporating some elements of the Sunrise process.

Section III: Relevant Resources

Name Collision Occurrence Management Framework: https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf [PDF, 926 KB]

gTLD Registry Agreement: http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

RPM Requirements: http://newgtlds.icann.org/en/about/trademark-clearinghouse/rpm-requirements-14may14-en.pdf [PDF, 387 KB]

Letter from the Registry Stakeholder Group (RySG), the Business Constituency (BC), and the Intellectual Property Constituency (IPC): https://www.icann.org/en/system/files/correspondence/cooper-et-al-to-chalaby-ngpc-17jul14-en.pdf [PDF, 153 KB]

Letter from the Internet Committee of the International Trademark Association (INTA): https://www.icann.org/en/system/files/correspondence/macpherson-to-chalaby-18jul14-en.pdf [PDF, 560 KB]

Section IV: Additional Information

Staff Contact

Karen Lentz
karen.lentz@icann.org