Comments of the Intellectual Property Constituency on the Draft Report on New gTLD Program Safeguards Against DNS Abuse

April 26, 2016

The Intellectual Property Constituency (IPC) appreciates this opportunity to comment on the Draft Report on New gTLD Program Safeguards Against DNS Abuse (Draft Report). The Draft Report was prepared by ICANN staff and reviews safeguards that were put into place to protect against DNS Abuse in new gTLDs.

The Draft Report explores nine safeguards implemented as part of the new gTLD program to protect against DNS Abuse. ICANN also asked four specific questions related to the safeguards. The IPC's responses to those questions, as well as the IPC's additional general comments on the Draft Report, are provided below.

I. General Observations

In addition to the four questions presented, the IPC notes that the Draft Report does not focus on several forms of abuse that all new gTLD registries are obligated at least to respond to – including use of domain names to facilitate piracy or counterfeiting. These (among others) are listed in Spec. 11, para. 3(a) – the Public Interest Commitments (PICs) included in every new gTLD registry agreement. The Draft Report refers to "the activities described within Spec. 11" as "an additional definitional framework for the CCT-RT as they refine the scope of their review."[1] We encourage the CCT-RT to recognize such PICs as an additional, and critical, "safeguard against abuse" in its review.

Similarly, while there is some discussion of the efforts of a few registries to create enhanced security environments,[2] there is no mention that many registries voluntarily adopted additional PICs that go beyond the baseline established by Specification 11, para. 3(a) as part of enhanced efforts to prevent their new gTLDs from becoming safe havens for perpetrators of piracy, counterfeiting, and other forms of intellectual property abuse. We believe that this aspect of new gTLD safeguards must be addressed in the final Report.

Further, the disclaimer at the bottom of page 7 of the Draft Report should be expanded to note that the Registration Abuse Policies Working Group predated the development of the new gTLD registry agreement by some time, and some of its observations regarding "use abuse" have been superseded by certain elements in the registry agreement, including such specified abuses as piracy and counterfeiting, which inherently involve issues concerning uses of domain names and not mere "registration" issues. Regardless of any limitations on ICANN's ability to "*regulate*" online content, ICANN certainly has a responsibility to ensure compliance with (and if necessary, to enforce) the terms of its contractual agreements with registries and registrars, which does not constitute "regulation."

---

[1] *See* Draft Report, p. 8.
[2] *See* id. at pp. 30-31.

Finally, some of the observations made about the forms of abuse that are discussed in the Draft Report may be equally applicable to the forms of abuse that are not discussed. For instance, on pages 13-14, the observations about phishing apply to forms of intellectual property abuse, such as piracy, counterfeiting, and cybersquatting as well – namely, that while the overall scope of such activities in the new gTLD space is still being evaluated, it is clear that the creation of numerous new gTLDs provides numerous additional spaces for bad actors to migrate their abusive activities. The IPC urges the drafters to include references to these forms of abuse in the final Report, as dealing with these types of abuse are clearly within ICANN's mission and mandate.

II. Summary of IPC Responses

- The IPC supports continued and improved procedures to vet potential registry operators to ensure that bad actors do not run new gTLD registries. In particular, the IPC recommends crafting the vetting criteria with an emphasis on identifying past cybersquatting behavior. The IPC also recommends criteria to evaluate principals, officers, and affiliated organizations of new gTLD registry candidates in order to ensure that operators are not permitted to use "shell" organizations to escape scrutiny during the application process.
- The IPC supports the use of DNSSEC deployment, wildcard prohibition, and removal of orphan glue records in order to ensure the integrity and utility of registry information. In addition, the IPC believes the ICANN community could benefit from stricter adoption standards of these safety measures, as well as improvements in the techniques used to protect registry data.
- The IPC continues to strongly support a requirement for all gTLD registry operators to maintain a "thick" WHOIS structure, with open access to complete and accurate domain name registration information for every domain name in every TLD registry.
- The IPC supports centralized zone file access in order to provide IP owners and other legitimate users of this information with a single portal from which to obtain data on infringing or abusive domain names, as well as potential registry agreement violations by registry bad actors.
- The IPC supports the requirement that registries and registrars maintain a single point of contact to document registry- and registrar-level abuses in order to streamline the process of identifying abusive domain name registration practices and remedying such abuse.
- The IPC supports mandatory use of an Expedited Registry Security Request (ERSR) process in order to enable registries to take decisive action to protect consumers and brand owners from security threats and other abuses to the DNS such as phishing, identity theft, distribution of malware, and other types of malicious activity and fraud directed at consumers.
- The IPC supports a draft framework for a high security zone (HSZ) verification program, but appreciates the fact that the ICANN community previously failed to achieve this. In light of these unsuccessful efforts, the IPC suggests reviewing earlier proposals made by the IPC and other stakeholders, followed if necessary by additional analysis on the challenges and issues raised previously by the ICANN community, including the ICANN Board's willingness to commit to administering an HSZ verification program, and the form such a program should take.

III. IPC Responses to The Four Questions Presented.

A. Question 1: How Do We Ensure That Bad Actors Do Not Run Registries?

1. Vet potential registry operators.

Vetting potential registry operators to ensure that bad actors do not run new gTLD registries is a critical threshold safeguard. The IPC provides some additional background context and comments regarding this safeguard below.

As noted in the Report, ICANN conducted background screenings as part of the new gTLD application Initial Evaluation process and, on some occasions, again during the contracting stage (generally in cases where the applicant had undergone changes to its officers and directors after the submission of the original application). The screenings applied to both the applying entity and the individuals named in the application, generally the officers and directors of the applicant entity or other high-level personnel with legal or executive authority over the applicant entity. The screenings focused on two areas: (1) general business diligence and criminal history, and (2) history of cybersquatting behavior. The criteria used for criminal history screening aligned with the "crimes of trust" standard often used in the banking and finance industry.[3]

In addition, ICANN reserved the right to deny an otherwise qualified application based on any information identified during the background screening process, including, for example, a final and legally binding decision obtained by a national law enforcement or consumer protection authority finding that the applicant was engaged in fraudulent and deceptive commercial practices.[4]

As ICANN recognized, such screenings are necessary to protect the public interest, including the interest of consumers and intellectual property owners vis-à-vis confusing, deceptive, or otherwise harmful registry practices.[5]

Although the screening process itself could likely be improved (for example, to avoid multiple re-screenings based on changes in personnel), according to the Report all applicants were "successfully" screened. However, the Report goes on to state that it may be "too soon" to determine whether screenings eliminated bad actors in practice, given that there is limited data on rejections of applicants based on background screenings as well as any terminations of registry agreements due to the registry's failure to eliminate bad actors from among its officers or directors. That said, the IPC strongly supports the criteria used to screen applicants, including the focus on prior cybersquatting activity.

While, according to the Report, it is "near impossible" to determine whether this safeguard had a deterrent effect on prospective applicants, the IPC assumes that potential applicants with a history of cybersquatting activity would not have attempted to navigate the application process, knowing that ICANN would screen for such activity, thereby preventing egregious actors from participating in the process.

Nonetheless, several registry operators passed background screenings but have perpetrated various practices of concern to the IPC, and which arguably raise the kind of consumer protection concerns the

---

[3] *See* ICANN, New gTLD Applicant Guidebook, 1-8, 1-21 - 1-22 (June 4, 2012).
[4] *See* id., at 1-24.
[5] *See* id., at 1-24 ("Background screening is in place to protect the public interest in the allocation of critical Internet resources. . . .").

background screenings were designed to prevent. As ICANN is aware, the IPC has previously raised substantial concerns regarding Vox Populi, the operator of the .SUCKS new gTLD, in connection with unfair pricing and other misleading or abusive marketing practices that discriminatorily target brand owners. Similarly, Top Level Spectrum, the operator of the .FEEDBACK new gTLD, has engaged in equally troubling dubious practices. Furthermore, as the IPC has previously noted,[6] many questions were raised regarding how applicants affiliated with Demand Media, whose subsidiary Demand Domains has lost over 30 UDRP cases, were able to pass ICANN background checks.[7]

Indeed, the ability for applicants to use affiliated shell companies as the actual applicant entity and thereby bypass substantial screening is an area that may require further examination. ICANN may want to consider exploring additional measures that could increase transparency about shell companies, their owners and key investors. On the other hand, ICANN should consider a balanced approach to ensure background screenings are not unduly burdensome or intrusive for applicants that are large, publicly-traded multi-national corporations.

In short, while background screenings appear to have initially prevented a substantial number of bad actors from becoming registry operators, there are clearly improvements worth exploring, and additional considerations that need to be made. ICANN should consider improvements both at the initial screening stage and after a registry operator begins operations to ensure practices do not run afoul of requirements the screening process was designed to prevent and to ensure new gTLD models truly serve the global public interest.

B. Question 2: How Do We Ensure Integrity And Utility of Registry Information?

1. DNSSEC deployment, wildcard prohibition, and removal of orphan glue records.

The second group of safeguards listed in the Draft Report deals with methods of "ensur[ing] integrity and utility of registry information." While the concept of "registry information" is not specifically articulated in the document, despite the fact that registries have a wide variety of "information" (e.g., WHOIS, billing data, etc.) that could be considered valuable, it will nonetheless be assumed for purposes of these comments that the primary source of "information" to be protected is the registry's zone file, which contains details about the online location identifiers (IP addresses, etc.) of domain names which that particular registry manages. Other forms of "information," while still certainly worth protecting are, at least to a certain extent, dealt with in other sections of the Draft Report (e.g., the Question 3 group of safeguards).

The Draft Report lists three specific safeguards that were to be used to "ensure" the integrity and utility of a registry's DNS data: First, to require a "demonstrated plan" for deployment of Domain Name System Security Extensions (DNSSEC) from each registry that has not already adopted it; second, to require registries to implement "appropriate controls" to prevent DNS "wildcarding"; and third, requiring registries to "provide a plan in their application" for removing so-called "orphan glue records."

The IPC has no issue with any of these techniques per se, and the benefits of each are well-documented and have been accepted by many throughout the ICANN Community. If anything, the IPC simply notes that these measures either: (i) do not go far enough (e.g., would benefit from stricter adoption

---

[6] *See, e.g.,* IPC Comments on the Draft New gTLD Program Implementation Review (Sept. 23, 2015).

[7] *See, e.g.,* Domain Incite, *ICANN Won't Say How Demand Media Passed Its New gTLD Background Check* (May 31, 2013). The IPC has previously commented on this issue.

standards); and/or (ii) may need to be supplemented with additional techniques that protect the data in other ways.

For example, simply requiring registries to have a "plan" for implementing these techniques does not seem to really "ensure" that they will actually be put in place and used regularly. In our view, to be true "safeguards," such "plans" should have specific commitments from the registry on resource allocation and — most importantly — reasonable timetables for completion. That said, data in the Draft Report appear to indicate that adherence to these measures is fairly strong among new gTLD registry operators.

Further, each of these listed safeguards "ensures" the integrity and utility of such data largely by preventing bad actors — whether outsiders or within the registry itself — from sabotaging certain DNS queries, presumably in hopes of redirecting unsuspecting users to malicious websites. While this is certainly a laudable goal, very little treatment is given in the Draft Report to more basic notions of "ensuring" that registry DNS data is useful and accurate to begin with, and does not become lost or corrupted over time. Inaccurate or malicious DNS data can create numerous problems (including, but certainly not limited to, intellectual property infringement) irrespective of how or when it enters into the DNS, which the Draft Report does not appear to discuss.

C. Question 3: How Do We Ensure More Focused Efforts On Combatting Identified Abuse?

1. Require "Thick" WHOIS records to encourage availability and completeness of WHOIS data.

The IPC continues to strongly support a requirement for all gTLD registry operators to maintain a "thick" WHOIS structure, as required by ICANN consensus policies.[8] The IPC supports open access to complete and accurate domain name registration information for every domain name in every TLD registry in order to facilitate the resolution of legal and other disputes related to the registration and use of the domain name.

Simplifying access to this information through mandatory implementation of thick WHOIS is helpful in addressing abuses of intellectual property in the DNS. It would enable quicker response and resolution when domain names are used for illegal, fraudulent, or malicious purposes.

Such mandatory implementation should also facilitate the adoption of Internationalized Domain Names (IDNs). With the increasing internationalization of the gTLD registrant pool and gTLD registration data, the WHOIS system faces difficult challenges about how registration data should be collected and displayed when provided by registrants whose primary languages use a script that does not employ Latin characters. Standardizing the collection and retention of this data at the registry level avoids a situation where this information is held by hundreds or thousands of registrars who may apply data collection or display standards inconsistently, and who will face little if any realistic prospect of enforcement to require them to follow a uniform approach.

Finally, centralizing such data would ensure that registrar failure or other technical failures not related to the registry would not disrupt access to registration data that may be needed to timely address DNS abuse, thus serving a key consumer protection function.

Currently, in the three gTLD domain name registries that still rely on the thin WHOIS model, domain name registration data is decentralized and held by the individual registrar sponsoring a particular registration. This leaves public access to this data vulnerable to registrar technical failure, insolvency, or

---

[8] *See* http://www.icann.org/en/groups/board/documents/resolutions-07feb14-en.htm#2.c.

simply non-compliance with its contractual obligations regarding WHOIS data. Centralization of this data via a thick WHOIS model would significantly lessen the contractual compliance burden, as well as providing a critical redundancy and additional back-up when WHOIS data is simply not accessible from the sponsoring registrar.

Third, IPC also notes the data thus far generated by the WHOIS Accuracy Reporting System and summarized on page 25 of the draft report. IPC has previously noted that "the ARS should discount proxy and privacy service records when analyzing the accuracy of WHOIS data. The failure to analyze the effect of proxy services in regard to both accuracy and contactability overstates the accuracy of WHOIS data and undermines the validity of the results set forth in the Report ."[9] However, even if the reported results are taken at face value, ICANN should certainly not be satisfied with a status quo in which the contact information appearing in WHOIS (whether thin or thick) is insufficient to be able to contact the registrant by e-mail more than one-eighth of the time, or by telephone more than one-quarter of the time. The CCT-RT should be considering ways to improve the accuracy of the data appearing in the thick WHOIS systems of the new gTLDs.

2. Centralize Zone File access to create a more efficient means of obtaining updates on new domains as they are created within each TLD zone.

Similarly, the IPC supports centralized zone file access because doing so creates a single portal from which intellectual property owners, among other potential legitimate users of such information, can obtain data on domain names that infringe their trademark rights, otherwise misappropriate their intellectual property, or commit other abuse in the DNS, including potential registry agreement violations by registry bad actors (for instance, through self-allocation and activation of more than the allowed 100 names in the TLD necessary for the promotion or operation of the TLD). Thus, a streamlined mechanism for accessing this data is of particular importance to intellectual property owners. Further, access to centralized zone files increases efficiency for Rights Protection Mechanism (RPM) service providers such as the Trademark Clearinghouse, which rely on zone files to provide ongoing notifications to brand owners regarding recently-activated domain names matching their Clearinghouse-recorded trademarks. Currently, the Clearinghouse relies on its own internal, automated mechanism to "scrape" the DNS in order to obtain this data. Scraping multiple zone files increases the likelihood of errors in this information, resulting in a decreased ability of Trademark Clearinghouse to provide this important service to brand owners. Brand owners in turn face an increased likelihood that abusive domain names may go undetected, which may result in harm to both brand owners and consumers alike.

3. Document registry- and registrar-level abuse contacts and policies to provide a single point of contact to address abuse complaints.

The IPC supports the requirement that registries and registrars maintain a single point of contact to document registry- and registrar-level abuses, as such a requirement streamlines the process of identifying abusive domain name registration practices and remedying such abuse. Such contacts must not only be publicly available and easily accessible, but must be responsive. Contacts are only the initial issue. Of equal if not greater importance, the registries must have policies for dealing with abuse complaints. The IPC supports the requirement that registries have policies. Unfortunately, the Draft

[9] http://forum.icann.org/lists/comments-whois-ars-pilot-23dec14/msg00006.html.

Report makes no recommendation beyond having a policy. Clearly, there should be minimum requirements for policies – for example, they should be clearly-stated, reasonable, timely and as uniform as possible. The next iteration of this report should include recommendations along these lines regarding the content and execution of registry abuse policies. Under the current model, cases of abuse at the registry level are identified and remedied on a case-by-case basis, and may not have the benefit of such policies. This is unacceptable. The IPC would also encourage registries to implement a system for tracking abuse complaints and their resolution, and taking steps to blacklist repeat bad actors within the registry, among other possible voluntary steps to increase the efficacy of abuse contact and monitoring.

We believe registrars should follow similar steps, as well. The Draft Report does not focus on Registrar abuse contacts and policies, although registrars are included in this recommendation on page 2 of the Draft Report (but curiously, not on page 27). Registrars are already required under the 2013 RAA to maintain a single point of contact for abuse complaints, so in that sense, this recommendation is already satisfied. However, the IPC concerns regarding short-comings in registrar policies for dealing with abuse are similar to those stated above with regard to registries. The IPC also notes with concern that there are currently no specific processes or dispute mechanisms that allow complaints against a specific registrar. Instead, the only recourse available to victims of abusive registration tactics at the registrar level is to file a complaint directly with ICANN Compliance. However, the IP owner is not meaningfully involved in the compliance process, has no opportunity to present evidence or arguments to counter the abusive behavior, and has no say in the outcome of any investigation by ICANN. The Draft Report should recommend that such a process be established, so that these issues are not solely handled by ICANN Compliance.

4. Provide an Expedited Registry Security Request Process to address security threats that require immediate action by the registry and an expedited response from ICANN.

The IPC supports mandatory use of an Expedited Registry Security Request (ERSR) process. Given the increasingly sophisticated nature of security threats to the DNS, more stringent requirements are necessary to prevent these abuses and to maintain the integrity of the DNS. This is especially so in cases where intellectual property rights are leveraged to perpetrate DNS abuses such as phishing, identity theft, distribution of malware, and other types of malicious activity and fraud directed at consumers. Requiring the use of an ERSR process would enable registries to take decisive action to protect consumers and brand owners facing these kinds of security and consumer protection threats.

D. Question 4: How Do We Provide An Enhanced Control Framework For TLDs With Intrinsic Potential For Malicious Conduct?

1. Draft framework for a high security zone verification program.

The answer to the fourth question, and the ninth recommendation, was to "create a draft framework for a high security zone verification program to establish a set of criteria to assure trust in TLDs with higher risk of targeting by malicious actors—e.g. banking and pharmaceutical TLDs—through enhanced operational and security controls."

It is well worth recalling that between 2009 and 2011, many members of the community, including the IPC, criticized ICANN's proposal for a purely voluntary HSZ framework in the new gTLDs, and proposed

several alternative approaches that would have more securely ensured broader protections for users of a wider range of new gTLDs. [10] IPC strongly urges the CCT-RT (as well as the relevant PDP working groups now considering the next new gTLD round) to review these criticisms and consider whether it would be prudent to heed them more fully in future rounds.

Instead, the High Security Top-Level Domain (HSTLD) Zone Working Group was formed in December 2009. The Draft Report fails to identify that the HSTLD Working Group – for a number of reasons – was unable to provide a consensus recommendation in its Final Report. Therefore, the goal of the ninth recommendation was never achieved. As identified in the Draft Report, there have been two measures to provide some degree of increased security in the new gTLD program. The first was ICANN's review of security related questions in the new gTLD application process. This appears to have been largely ineffectual, as very few new gTLD applicant adopted security measures similar to criteria set forth in the HSTLD Working Group's Final Report. The second measure was through objections raised by the Government Advisory Committee (GAC). These led to the additional new gTLD safeguards embodied in the Public Interest Commitments (PICs), as discussed above. However, the GAC's additional concerns about security in certain "highly regulated sectors" have been implemented on an ad hoc basis, with no specific ICANN requirement obligating registry operators to adopt many of the proposed measures, causing some degree of uncertainty for new gTLD applicants. That said, many new gTLD registry operators of "high risk" strings have voluntarily implemented certain heightened security measures through registrant eligibility criteria and other registry policies.[11]

There is no doubt that ICANN failed to fulfill the ninth recommendation to create a high security zone verification program. The Draft Report suggests that the Competition, Consumer Choice, and Consumer Trust Review Team (CCT-RT) collect "feedback from registry operators on why they chose not to pursue high security zone (HSZ) verification[, which] could provide insight into this recommended safeguard's lack of adoption. Also, speaking with the fTLD Service, LLC registry on why they chose to pursue their own HSZ could provide an additional source of data."

As an initial matter, the IPC agrees that CCT-RT ought to discuss the experience of fTLD in launching its .BANK and .INSURANCE new gTLDs. However, a flaw in the report's recommendation is that it presumes there was some specific form of "HSZ verification" that registry operators could have adopted. In

---

[10] See, e.g., https://archive.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf, at 34-35 (summarizing comments on Draft Applicant Guidebook v. 3); http://ipconstituency.org/PDFs/2009_Nov22_IPC_comments_on_mitigating_malicious_conduct.pdf, at 1 ("all proposed mechanisms designed to mitigate malicious conduct should be considered required elements of the new gTLD program, not voluntary options "); (http://www.onlineaccountability.net/assets/2010_Jul21_COA_Comments_DAGv4.pdf, at 10-11 (comments of IPC member COA on Draft Applicant guidebook v.4, proposing three alternative approaches to achieving stronger incentives for increased security within new gTLDs); http://static1.1.sqspcdn.com/static/f/585526/26639784/1446229403480/1.+IPC+Comments+on+the+Proposed+Final+New+gTLD+Applicant+Guidebook+2010_12December_09.pdf?token=qPo9%2B8F%2FWOFlEpNHBAmmGl5zFsQ%3D , at 11, IPC Comments on Proposed Final Version of Applicant Guidebook ("the requirement for … higher level enhanced protections commensurate with the nature of the applied-for gTLD string [should apply] to gTLDs in other areas, including health care-related TLDs, TLDs directed to children, and all TLDs that present an unusually high risk of being the venue for criminal, fraudulent, or illegal conduct, including but not limited to copyright piracy, trademark counterfeiting, or other forms of intellectual property theft").

[11] *See, e.g.*, fTLD Service, LLC, Registrant Eligibility Policy (Dec. 17, 2014) (limiting registrant eligibility to certain businesses and organizations subject to certain government oversight).

reality, a close reading of the HSTLD Working Group's Final Report suggests that it could never reach consensus for fundamental reasons that were outside of the community consensus for an HSZ verification program. Specifically, it appears that (a) ICANN would not agree to be a certifier, (b) a business case could not be made for third-party certifier to operate the program, and (c) registries did not want a mandatory certification program because it would add operational costs.

In light of these facts, the IPC would suggest the following additional analysis be undertaken by the CCT-RT, but only after completing a review of the proposals (made by IPC and others) for a stronger and more comprehensive program that were rejected by ICANN in preparing the current round:

- Recommendation No. 1: CCT-RT needs to get true buy-in from the ICANN Board that ICANN is willing to take on the responsibility of administering an HSZ verification program.
- Recommendation No. 2: The CCT-RT should use the data that it collects to make recommendations or even determinations concerning the following issues:
    - Should the HSZ verification be mandatory or voluntary?
    - Should the HSZ verification be limited to certain classes of names?
    - How should HSZ verification impact a new gTLD application scoring?
    - How far should the HSZ verification extend (Registry, Registrar, Registrants, Website operators, Browsers)?
    - How can an HSZ verification program positively impact the other 8 recommendations?

The HSTLD WG recommended that a working group comprised of experts should be formed to continue work on an HSZ verification. Should the CCT-RT analysis indicate that an HSZ verification program is viable, the IPC encourages the CCT-RT to make a recommendation for the formation of this new working group.

Respectfully submitted,

Intellectual Property Constituency