

## Registries Stakeholder Group Statement

Issue: **Competition, Consumer Trust and Consumer Choice Review Team (CCTRT) Final Report & Recommendations**

Date statement submitted: **11 December 2018**

Reference URL: <https://www.icann.org/public-comments/cct-final-recs-2018-10-08-en>

### Background<sup>1</sup>

Topics covered in the report:

New gTLD Program history	DNS Abuse	Right Protection Mechanisms
Competition in the DNS Marketplace	Safeguards	Application and Evaluation
Consumer Choice	DNS Security Abuse	Trademarks
Consumer Trust	Public Interest Commitments	

The Report contains **35 recommendations**, the RT indicated whether implementation is prerequisite or added a time-bound priority level:

- **Prerequisite:** Per the ICANN Bylaws, RT indicates whether implementation must be prior to the launch of subsequent procedure
- **High priority:** Must be implemented within 18 months of the issuance of a final report
- **Medium priority:** Must be implemented with 36 months of the issuance of a final report
- **Low priority:** Must be implemented prior to the start of the next CCT Review

Overall conclusion:

*“Initial indications are that the New gTLD Program has led to a dramatic increase in consumer choice, a modest, but important, increase in competition, and has had a minimal impact on consumer trust. However, there are several TLDs with a disproportionate level of DNS security abuse and the review team recommends enhancements to various enforcement mechanisms prior to any further additions to the DNS. The review team believes that there is a substantial need for more and better data on both competition and pricing, and on the impact of safeguards on consumer protection.*”

The RySG commented on draft version of the report and recommendations:

- RySG Comment on the CCTRT - Draft report on Recommendations (19 May 2017)  
[https://docs.wixstatic.com/ugd/ec8e4c\\_48249938cc36403dbdfe9582a6657d34.pdf](https://docs.wixstatic.com/ugd/ec8e4c_48249938cc36403dbdfe9582a6657d34.pdf)
- RySG Comment on the CCTRT - new sections to draft report (15 January 2018)  
[https://docs.wixstatic.com/ugd/ec8e4c\\_ff7158c0470f40bc89c8c6ae2f8f5e03.pdf](https://docs.wixstatic.com/ugd/ec8e4c_ff7158c0470f40bc89c8c6ae2f8f5e03.pdf)

---

<sup>1</sup> *Background:* intended to give a brief context for the comment and to highlight what is most relevant for RO's in the subject document – it is not a summary of the subject document.

## Registries Stakeholder Group Comment:

### **Introduction & Overarching Comments**

The Registries Stakeholder group thanks the CCT-RT for its work and thanks the Board for an opportunity to comment. We have deep concerns with this Final Report. Most of its recommendations are overbroad, unsupported by data, or fiscally irresponsible, and many violate the terms of our contracts with ICANN. We raised these concerns in our first and second public comments. The CCT-RT appears to either not have considered them or have disregarded them without a rationale as its Final Report contains no substantive reference to them.

We urge the Board not to adopt the Recommendations wholesale. We urge you to critically review the Recommendations in light of our comments and adopt only the ones that are fully within ICANN's remit and are likely to provide significant, meaningful data that will yield measurable results. Some of the Recommendations may need to be altered by the Board before they can be adopted. Some should not be approved at all.

ICANN must manage to its budget. Recommendations that are unworkable and overbroad will waste the community's resources and the Final Report has not identified how it will fix the gaps we identified in the previous public comments we submitted on the CCT-RT's Initial and Supplementary reports. Significantly, all of the Recommendations have the following theme: they aim to restrict what registry operators can do until we are all following the same model. In addition to limiting meaningful competition and suppressing innovation, the Final Report further intends to hold registry operators accountable for all downstream uses of our services while micromanaging pricing. We will not repeat our earlier public comments because we urge the Board to read them in full. For convenience, our comment is formatted so that each RySG response immediately follows the related Recommendation. We summarize our top concerns by topic below.

#### *Violate Registry Contracts*

The Final Report recommends that ICANN compel registry operators to negotiate both incentives,<sup>2</sup> and penalties,<sup>3</sup> for proactively monitoring for abuse as well as specific user protections for a registrant's customers. The Bylaws prohibit regulating content,<sup>4</sup> and abuses not already covered by our registry agreements are generally content-based abuses, such as cyberbullying<sup>5</sup>, or business-based abuses, such as a website operator's mishandling of their own customer data<sup>6</sup>. The Final Report further suggests ICANN Compliance should be used to gather data from registries that is not required under our contracts.<sup>7</sup>

---

<sup>2</sup> Recommendation 14. To be clear, some registry operators may not object to incentives to proactively monitor abuse, but Recommendation 19 is a classic example of what happens when we voluntarily come to the table.

<sup>3</sup> Recommendation 15.

<sup>4</sup> ICANN Bylaws, Article 1.1(c).

<sup>5</sup> Recommendation 24. Cyberbullying is website content and is not related to the registration of a domain name.

<sup>6</sup> Recommendation 13(3) and Recommendation 22 suggest a registry operator should be responsible for a registrant's customer's sensitive data.

<sup>7</sup> See Details for Recommendation 13 (none of the data requests in the Recommendation are part of any registry agreement, absent a PIC). In addition to implying Contractual Compliance should have an expanded role, the Final Report directly states "...Contractual Compliance is expanding its audit functions to include additional examination of compliance with certain safeguards." Details for Recommendation 23.

### *Overbroad*

The Final Report adopts the narrow thinking that if a business practice is good for some registry models, it should be applied to all registries. This one-size-fits-all approach is precisely what many new gTLD applicants were trying to avoid because it stifles creativity and innovation. Several recommendations call for data in order to determine if some registry business decisions (like price, customer terms, or registration eligibility restrictions) should be applied to all registry operators, regardless of business model.<sup>8</sup> We urge the Board to protect the innovations both new and legacy TLD operators, and our registrar partners, are trying to bring to the DNS rather than assuming the industry is static. Forcing us all into one model will prevent the next “big thing”.

### *Assumptions unsupported by data*

The same narrow thinking causes the Final Report to imply that price<sup>9</sup> is the key to evaluating competition and choice. Registry operators offer consumers choice on more than just price. Yet the only Recommendations about competition turn on how much money everyone in the supply chain is selling domains for, assuming that lower prices are the only measure of competition. Similarly, Recommendation 27 requests that the RPMs PDP evaluate four suggestions to change the URS without identifying what problems prompted the recommendations and how the Final Report determined that those four recommendations were the solution to the problem.

### *Fiscal Responsibility*

Throughout the report, the CCT-RT recommends data-gathering projects, surveys, and studies assuming that anywhere they don't have data is a problem. The RySG urges the Board to balance the perceived benefit of expensive and time-consuming data gathering exercises against the anticipated cost and synthesis of all the data. Some recommended studies, while potentially yielding fascinating information, are highly unlikely to have any significant outcome that will influence the next round of applications.<sup>10</sup>

As the Board is aware, the Registries Stakeholder Group is made up of over 70 registry operators with contracts for several hundred TLDs, each with a vast array of interests and business models. We are actively involved in ensuring ICANN and the DNS are trusted, secure and stable. Domain names are our business. No one wants them to be viable and succeed more than we do. We agree that a periodic review of the state of the system through a CCT-RT is a good thing, but we have deep concerns that many of the Recommendations would be irresponsible for ICANN to adopt as written. We ask the Board to tailor its response to this report to ensure that the projects that flow out from out from it are measured, cost-effective, realistic, and within ICANN's remit.

---

<sup>8</sup> See Success Measures for Recommendation 11 and Recommendations 12 and 13. See also Recommendation 9, which suggests an entirely new RPM (as a prerequisite to the next round) especially for the trademark holders who have elected to participate in the new gTLD system through the TMCH or Sunrise.

<sup>9</sup> Recommendations 2, 3, 4, and 5.

<sup>10</sup> Recommendations 5, 7.

## Comments on the Recommendations

### Chapter V. Data-Driven Analysis:

#### Recommendations for Additional Data Collection and Analysis

<b>Recommendation 1.</b> <b>Formalize and promote ongoing data collection.</b>		
<p><b>Rationale/related findings:</b> The lack of data has handicapped attempts both internally and externally to evaluate market trends and the success of policy recommendations.</p> <p><b>Details:</b> In an effort to promote more objective policy development inside ICANN, the ICANN organization should establish a formal initiative, perhaps including a dedicated data scientist, to facilitate quantitative analysis of policy initiatives and reviews by staff, contractors, and the community. Specifically, where possible, the ICANN organization should proactively collect data needed to validate or invalidate policy initiatives (whether ICANN organization- or community-driven), identify and collect data necessary to measure program success, both incrementally and in retrospect. On a case-by-case basis, this initiative would help to ascertain the cost/benefit and security requirements for the data in question.</p> <p><b>Success Measures:</b> The ability for the community to determine, through review process, if policy initiatives had well-defined issue measurement to justify reform and facilitate review.</p>	<p><b>To</b> ICANN organization</p>	<p><b>Priority level</b> High</p>
<p><u>2017 RySG comment:</u> This, according to the RT’s rationale, is an extremely wide-ranging recommendation—it advocates for data collection regarding multiple market sectors, the impact of safeguards, compliance information, and other material. While we are in favor of reasonable levels of market intelligence that can more precisely inform policymaking (corollary: we support data-based reports on the outcomes of policy implementation), there are 23 pages of rationale supporting this recommendation. The community would be well served to carefully review this practically open-ended request and consider each category judiciously. In fact, it may be wise to separate the categories detailed in the rationale into separate recommendations in order to better address each.</p>		
<p><u>RySG comment:</u> The RySG reiterates its 2017 comment. The CCT-RT kept the 23 pages of rationale, which include multiple statements of opinion, and did not heed the RySG’s advice to narrowly tailor the request for data by categories. As a result, this recommendation lacks the specificity needed for the Board to act.</p>		

## Chapter VI. Introduction to the Competition and Consumer Choice Analysis

<p><b>Recommendation 2:</b>  <b>Collect wholesale pricing for legacy gTLDs.</b></p>		
<p><b>Rationale/related findings:</b> The lack of data from legacy gTLDs and transactional data will continue to hinder future CCT Review Teams' efforts to analyze competition between registries in the domain marketplace. In particular, the review team was unable to determine whether wholesale prices charged by legacy gTLDs had declined as a result of increased competition due to the introduction of new gTLDs.</p> <p><b>Details:</b> ICANN could work with an appropriate contractor and registry operators to acquire wholesale price information from both legacy and new gTLD registries on a regular basis, including at least a sample of transactional data. Transactional data is essential to allow analysis of the cost of similar strings across TLDs, and to understand the role of promotional pricing by registries. Due to the sensitive nature of this data, ICANN should provide strong assurances that the data would be treated on a confidential basis, including collecting the data under a nondisclosure agreement. In the event that ICANN is unable to establish a voluntary framework for sharing this information, this may require amendment to the Base Registry Agreement for legacy gTLDs.</p> <p><b>Success Measures:</b> The ability for a third-party economic study to establish a meaningful understanding of (1) wholesale pricing in legacy gTLDs; (2) the role of promotional pricing in the marketplace; and (3) the value of individual second-level labels across various TLDs.</p>	<p><b>To</b>  ICANN  organization</p>	<p><b>Priority level</b>  Low</p>
<p><u>Updated 2017 RySG comment:</u> In its current form, this recommendation is not supportable:</p> <ul style="list-style-type: none"> <li>· Price information generally is business sensitive.</li> <li>· “Strong assurances” is ill defined and, should this recommendation be considered, would need to be presented in detail to registries and registrars, with their extensive input on handling of data.</li> <li>· “Confidential basis” does not specify who would have access to data.</li> <li>· “Analytic purposes” also would need to be much more clearly defined, and a statement of eventual outcome elucidated.</li> <li>· Non-disclosure agreements are helpful, but it isn’t clear who would arbitrate access to the data, and to what extent.</li> </ul>		
<p><u>RySG comment:</u>  We reiterate the statements we made in 2017, with an edit to reflect the changed ‘details’ accompanying the recommendation (see above). The rationale provided does not indicate any valid basis for requesting registry wholesale pricing. The recommendation appears to infer that lower legacy prices might indicate more competition, but this is an unsupported hypothesis and this recommendation comes off as a “fishing expedition” for sensitive data. Furthermore, the CCT-RT suggests that ICANN should compel legacy TLD operators to the table to negotiate a contract amendment in order to forcibly obtain information to which ICANN and the community are not otherwise entitled.</p>		

**Chapter VI. Introduction to the Competition and Consumer Choice Analysis**

<p><b>Recommendation 3:</b>  <b>Collect transactional pricing for the gTLD marketplace.</b></p>		
<p><b>Rationale/related findings:</b> The lack of transactional data will continue to hinder future CCT Review Teams’ efforts to analyze competition between registries in the domain marketplace. Although ICANN was able to obtain base wholesale prices from registries, individual domain transactions are often sold at either a significant discount as part of promotional campaigns, or at a significantly higher price than the baseline price for certain premium domains. For some TLDs, the review team believes that a large fraction (even a substantial majority) of domains were sold at discounted prices. Therefore, any pricing analysis based solely on the base wholesale price is unlikely to correctly capture the competitive dynamics in the marketplace.</p> <p><b>Details:</b> ICANN or an outside contractor should attempt to acquire at least some samples of wholesale price information from registries on a regular basis and provide necessary assurances that the data would be treated on a confidential basis. The data could then be used for analytic purposes by the ICANN organization and by others that execute non- disclosure agreements.</p> <p><b>Success Measures:</b> The availability of relevant data for use by the ICANN organization, contractors, and the ICANN community for its work in evaluating competition in the DNS marketplace.</p>	<p><b>To</b>  ICANN  organization</p>	<p><b>Priority level</b>  Medium</p>
<p><u>2017 RySG comment:</u> For many of the reasons cited in our reply to recommendation 2, this recommendation cannot be supported. “Analytic purposes” does not remotely suggest a well considered benefit to ICANN, registries or the community, particularly given ICANN’s lack of remit over pricing.</p>		
<p><u>RySG comment:</u>  We reiterate our 2017 comment and additionally note:</p> <ol style="list-style-type: none"> <li>1. This recommendation for “transactional data” for “individual domain transactions” does not match the Detail section which again asks for wholesale pricing.</li> <li>2. The definition of success is overbroad and not narrowly tailored to achieve a defined purpose.</li> <li>3. This entire section is worded in the passive voice. Who shall gather this data, and from whom? Will ICANN spend millions to track down end users and compel them to disclose what they paid? A significant portion of domain names sold are not even sold by contracted parties but are sold by resellers or in private sales and auctions.</li> </ol>		

## Chapter VI. Introduction to the Competition and Consumer Choice Analysis

<p><b>Recommendation 4:</b>  <b>Collect retail pricing for the domain marketplace.</b></p>		
<p><b>Rationale/related findings:</b> The lack of retail data will continue to hinder future CCT Review Teams' efforts to analyze competition between registries and TLDs in the domain marketplace. One of the anticipated benefits of increased competition from the introduction of new gTLDs would be lower prices for registrants of domain names. Prices charged by registrars to registrants are the best indicator of this potential consumer benefit. In addition, retail prices offered to the public will generally be accessible through registrars' public websites and will not require additional disclosures to ICANN by contracted parties. (Note that some registrars, such as those providing corporate/brand protection services, do not publish their prices and therefore would not be represented in a survey of publicly available prices.)</p> <p><b>Details:</b> ICANN does not currently make use of retail price data that can be obtained directly from public sources such as <a href="https://tld-list.com/">https://tld-list.com/</a> and <a href="https://namestat.org">https://namestat.org</a>. We recommend that ICANN develop the capability to analyze these data on an ongoing basis. Alternatively, an amendment to the Registrar Accreditation Agreement would ensure the availability of this data with all due diligence to protect competitive information.</p> <p><b>Success Measures:</b> The availability of relevant data for use by the ICANN organization, contractors, and the ICANN community for its work in evaluating competition in the DNS space.</p>	<p><b>To</b>  ICANN  organization</p>	<p><b>Priority level</b>  Low</p>
<p><u>2017 RySG comment:</u> Registries don't purport to speak for registrars; however, we're confident we share a concern that not only should ICANN not involve itself with pricing studies, using parties' contracts with ICANN as a mechanism to force its production is terribly inappropriate. Contracts are not levers for mandatory revelation of sensitive data.</p>		
<p><u>RySG comment:</u>  In addition to reiterating our 2017 comment, the RySG notes that the CCT-RT's narrow focus on price as the chief indicator of competition is short-sighted and misses many other ways registries and registrars compete. By focusing on price alone, you're missing the value of the domain name ecosystem.</p>		

## Chapter VI. Introduction to the Competition and Consumer Choice Analysis

<b>Recommendation 5:</b> <b>Collect secondary market data.</b>		
<p><b>Rationale/related findings:</b> The presence of price caps in certain TLDs hinders efforts to comprehensively analyze competitive effects. The true market price may very well be above the caps. Accordingly, the secondary market is the best place to see price movement.</p> <p><b>Details:</b> ICANN should engage with the secondary market community to better understand pricing trends. Ideally, ICANN would be able to be able to obtain long-term transactional data that would allow it to evaluate whether the price of similar domain names was increase or decreasing over time, and whether there was any relationship to the introduction of new gTLDs. Given that it may be difficult to obtain such data, aggregated data that show per-TLD trends or overall trends in market pricing that take into consideration the introduction of new gTLDs would still be an improvement over the current limited data on pricing dynamics in legacy gTLDs.</p> <p><b>Success Measures:</b> The availability of relevant data for use by the ICANN organization, contractors, and the ICANN community for its work in evaluating competition in the DNS space.</p>	<b>To</b> ICANN organization	<b>Priority level</b> High
<p><u>2017 RySG comment:</u> The RySG repeats its concern over any ICANN interest in pricing. The secondary market is once removed from the primary market and is even further outside ICANN's remit. In addition, except for publicly reported transactions, it likely would be very difficult to convince parties to private transactions to divulge sales prices. What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?</p>		
<p><u>RySG comment:</u> The RySG reiterates its 2017 comments.</p>		



## Chapter VI. Introduction to the Competition and Consumer Choice Analysis

### Recommendation 6:

**Partner with mechanisms and entities involved with the collection of TLD data. As feasible, collect TLD registration number data per TLD and registrar at a country-by- country level in order to perform analysis based on the same methods used in the LAC study.**

**Rationale/related findings:** The lack of country-level data will continue to frustrate future CCTReview Teams' efforts to analyze competition between registries and TLDs in the domain marketplace. In particular, the lack of country-specific data hinders efforts to understand the competition between gTLDs and ccTLDs. ccTLD data, which is useful in understanding the overall TLD marketplace, is particularly hard to come by.

**Details:** Some of this data is collected by third parties such as CENTR, so it is possible that ICANN can arrange to acquire the data.

**Success Measures:** The availability of relevant data for use by the ICANN organization, contractors, and the ICANN community for its work in evaluating competition in the DNS space.

**To**  
ICANN  
organization

**Priority level**  
Low

2017 RySG comment: Before any work of this nature is undertaken, it is essential that a statement of benefit is clearly articulated and that the costs of undertaking the work are well defined and measured against the statement of benefit  
The RySG is concerned that such an undertaking may be expensive in terms of financial and/or other ICANN resources and that resource allocation in this area may impact on critical policy or other ICANN priorities.  
ICANN serving as a coordinator of research, standardizing methodology, and directing resources toward organizations *already* involved in such research may be practical and beneficial.  
However, without a clear statement of benefit, method and cost, it is not sufficiently well justified (making it unclear why this is labelled as prerequisite). Our question is therefore: What is the perceived benefit of this recommendation, what would the method and cost be to undertake it, and would the benefit exceed the cost?

RySG comment:

The RySG reiterates its 2017 comments.

## Chapter VI. Introduction to the Competition and Consumer Choice Analysis

### Recommendation 7:

#### Collect domain usage data to better understand the implications of parked domains.

**Rationale/related findings:** The high incidence of parked domains suggests an impact on the competitive landscape, but insufficient data hinders efforts to analyze this impact.

**Details:** The review team uses the term “domain usage” rather than “parking” in the recommendation because the term “parking” is associated with a wide variety of behaviors, and different members of the community may define “parking” differently. It is also likely that different types of “parking” behaviors reflect different intentions by registrants and will have different implications on the competitive dynamics in the marketplace. ICANN should regularly track the proportion of domains in gTLDs that are parked with sufficient granularity to identify trends on a regional and global basis. Ideally, data would allow analysis to occur on a per-domain basis rather than being aggregated on a TLD level. Future reviews should conduct further analyses of whether there is a correlation between parked domains and renewal rates or other factors that may affect competition. Further analysis should be performed on the relationship between parking and DNS abuse. The community may also wish to take this issue up for further study outside of the periodic CCT Review process, as the phenomenon is also prevalent within legacy gTLDs, and there does not seem to be significant study of the topic with ICANN.

**Success Measures:** The availability of relevant data for use by the ICANN organization, contractors, and the ICANN community for its work in evaluating competition in the DNS space.

**To**  
ICANN  
organization

**Priority level**  
High

2017 RySG comment: The RySG obviously is in favor of increasing usage. However, while this data could be useful, it’s unclear how, in the end, it would be put to use by the ICANN organization or the community.

Jan 2018 RySG comment: The various studies that the CCT-RT undertook to measure the impact of parking on both competition and rates of DNS abuse returned inconclusive results. The new sections of the report put forth a number of possible hypotheses that could be explored, but which have no demonstrable, concrete bases. Given the absence of a documented problem, the RySG believes additional studies on parking are unnecessary at this time and are an ineffective use of ICANN’s shrinking resources.

To the extent ICANN adopts this recommendation and dedicates resources to study parking further, the RySG recommends that ICANN take a critical approach and scrutinize the utility and validity of those studies, without pre-supposing the outcomes of any studies.

RySG comment:

The RySG reiterates its 2017 and 2018 comments.

## Chapter VII. Consumer Choice

### Recommendation 8:

**Conduct periodic surveys of registrants that gathers both objective and subjective information with a goal of creating more concrete and actionable information.**

**Rationale/related findings:** Although Nielsen conducted two surveys of registrants in conjunction with the CCT, the set of questions posed did not allow for a full analysis of consumer motivations or to understand how valuable they found the expanded choice offered by the new gTLDs. At the same time, as the review team observed additional registrations and more familiarity with new gTLDs, it is likely that consumer attitudes will change over time as well. A periodic survey will allow the community to observe those changes.

**Details:** Because the survey supports further analysis of both consumer choice and consumer trust, it must pose questions relating to both topics. In both cases, it is important to know which TLDs consumers are familiar with and which they actually visit.

To better understand issues of consumer trust, it is also important to understand why they choose to register in some TLDs but not others, and whether the TLD's registration policies and perception of trustworthiness influence the choice of whether or not to register.

For consumer choice, the survey should allow a relative weighting of the potential contributions to consumer choice with respect to geographic name gTLDs, specific sector gTLDs, and IDN gTLDs. The survey should help determine whether there is a clear preference by registrants for different types of gTLDs and whether there are regional differences or similarities in their preferences. It will also be important to gather further data on geographic distribution of gTLD registrants and the services provided to them by registrars, particularly in different regions, including languages offered for service interactions and locations beyond primary offices.

The survey should be designed to repeat portions of previous surveys while continuously striving to improve the data available on registrant behavior and attitudes. Some potential questions are included in Appendix G: Possible Questions for a Future Consumer Survey. The survey should allow an analysis of: (1) what factors matter most to users in determining which gTLDs to visit; (2) whether perceived trustworthiness of TLDs influences registration behavior; (3) the the perception of new gTLDs with restrictions on registration compared to new gTLDs with few or no restrictions; and (4) whether registrants view the expanded name space as beneficial or confusing.

**Success Measures:** The availability of relevant data for use by the ICANN organization, contractors, and the ICANN community for its work in evaluating competition in the DNS space.

**To**  
ICANN  
organization

**Priority level**  
Low

RySG comment 2017: What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

#### RySG comment:

The RySG reiterates its 2017 comment. Additionally, the RySG believes the proposed questions in Appendix H (not G) are too narrow, speculative, and leading to result in meaningful answers. The CCT-RT should clearly lay out the information it seeks to and then let a qualified survey provider determine which questions, including follow-up questions, will get at the data likely to provide that information. For example, Q1 might simply ask "what are switching costs" (keeping in mind that the CCT-RT itself notes slightly later in the survey that most businesses with a TLD on a legacy page don't simply "switch" to a new gTLD but likely use a slow phase-in and maintain dual sites for years, if not forever)?

**Chapter VII. Consumer Choice**

**Recommendation 9:**

**The ICANN community should consider whether the costs related to defensive registration for the small number of brands registering a large number of domains can be reduced.**

**Rationale/related findings:** The review team found that while most trademarks were either not registered in new gTLDs or in only a handful of new gTLDs, a small number of trademarks were responsible for a large number of registrations across many new gTLDs and were likely bearing most of the cost of registrations. This bimodal distribution suggests that RPMs tailored to certain of these trademarks may be appropriate.

**Details:** The review team does not suggest a specific mechanism. However, the review team believes the uneven distribution of costs of defensive registrations to a small number of trademark holders may be an unanticipated effect of the current RPM regime and that the relevant PDP(s) should consider whether those costs can be lowered without impacting the benefits of the New gTLD Program, thereby improving the cost-benefit ratio of the overall Program.

**Success measures:** A reduction in the number of defensive registrations overall and, in particular, a reduction in the number of defensive registrations per trademark by the registrants with the most defensive registrations without causing an increase in the number of UDRP and URS cases.

**To**  
Subsequent Procedures  
Policy Development  
Process (PDP) Working  
Group and/or Rights  
Protection Mechanisms  
(RPM) PDP Working  
Group

**Priority level**  
Prerequisite

2017 RySG comment: What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

RySG comment:

The RySG believes this data is at best elusive and more likely impossible to get, given the reluctance of corporations to provide such confidential business information. Furthermore, the wording “uneven distribution costs of defensive registrations to a small number of trademark holders” implies that the trademark holders themselves have no say on the size of their defensive registration budgets and portfolios, whereas in reality, some may simply be more risk-averse than others. Given the futility of this exercise, the RySG reiterates its 2017 comment and strongly objects to this work being a prerequisite for another round.

## Chapter VII. Consumer Choice

### Recommendation 10:

The GNSO should initiate a new Policy Development Process (PDP) to create a consistent privacy baseline across all registries, including to explicitly cover cases of privacy infringements such as sharing or selling personal data without a lawful basis, such as the consent of that person. The GNSO PDP should consider limiting the collection and processing of personal data within rules which are mandatory for all gTLD registries. It should also consider not allowing registries to share personal data with third parties without a lawful basis, such as the consent of that person or under circumstances defined by applicable law (e.g. upon requests of government agencies, IP lawyers, etc.). Also, it is necessary to be aware of emerging, applicable regulations related to the processing of the personal data. For clarification, this recommendation does not relate to issues involving WHOIS or registration directory services data.

**Rationale/related findings:** As mentioned above, the policies of the top 30 new gTLDs have rules regarding sharing of personal data of its registrants with third parties. Furthermore, some of those policies have very clear statements that registries have the right to share or sell personal data.

**Details:** Despite the fact that the Base Registry Agreement has references to privacy laws and policies, some of the registries are explicit that they have right to share personal data with third parties without consent of that person or under circumstances defined by applicable law.

**Success measures:** The development of relevant policy and update of the Base Registry Agreement.

To  
GNSO

Priority level  
Medium

### RySG comment:

The RySG notes that the expected outcome of the EPDP is a permanent data privacy/protection specification, including strict purposes for which registries and registrars may transfer or share data. To the extent that this recommendation applies to privacy outside of WHOIS/RDDS data, the RySG questions whether such policies or “baselines” fall within the picket fence and are an appropriate subject for a PDP.

**Chapter VIII. Consumer Trust**

**Recommendation 11:**

**Conduct periodic end-user consumer surveys. Future review teams should work with survey experts to conceive more behavioral measures of consumer trust that gather both objective and subjective data with a goal toward generating more concrete and actionable information.**

**Rationale/related findings:** The New gTLD Program is still in its early days. In order to further analyze consumer choice and trust, surveys of consumer end-users must be continued in order to better understand their behavior and motivations.

To better understand issues of consumer trust, it is also important to understand why consumer end-users choose to visit some TLDs but not others; whether the TLD’s registration policies influence the choice of whether or not to visit; and whether consumer end-users behavior on certain websites indicate varying levels of trust across TLDs.

For consumer choice (discussed above), the survey should allow a relative weighting of the potential contributions to consumer choice with respect to geographic name gTLDs, specific sector gTLDs, brand gTLDs, and IDN gTLDs to help determine whether there is a clear preference among consumer end-users for different types of gTLDs, and whether there are regional differences or similarities in their preferences.

**Details:** Future review teams should work with survey experts to conceive more behavioral measures of consumer trust that gather both objective and subjective data, with a goal toward generating more concrete and actionable information. In addition, the survey should repeat applicable parts of the global surveys for consumer end-users to allow an analysis of (1) which new gTLDs they have visited most; (2) the reasons they give to explain why they visited certain new gTLDs more than others; (3) what factors matter most to them in determining which gTLDs to visit; (4) how their behaviors indicate to what extent they trust new gTLDs; (5) the trustworthiness of new gTLDs with restrictions on registration compared to new gTLDs with few or no restrictions; and (6) whether consumer end-users view the expanded name space as beneficial or confusing.

**Success measures:** This recommendation would be considered successful if it produces data that enables future review teams and the ICANN organization to see how the levels of trustworthiness correlate with the number of visitations to new gTLDs, and what factors may contribute to the levels of trustworthiness. For example, registration restrictions appear to contribute to higher levels. This information could inform future policy-making on the terms and conditions that should apply for all new gTLD applicants. Another success measure would be information for new gTLD applicants in regard to what factors may lead to increased visitation and trustworthiness for new gTLDs. The last success measure would be data that informs ICANN policy on registration restrictions, especially if the data indicates that certain basic restrictions enhance trustworthiness in the gTLD space, alongside other variables driving gTLD model design and diversity. Those applicants choosing to apply for gTLDs with restrictions would then have a better basis for the decision to do so.

**To**  
ICANN organization  
and future CCT Review  
Teams

**Priority level**  
Prerequisite

RySG comment 2017: The RT’s rationale states that the findings of such a study could help measure the extent of trust the public places in new gTLDs, and that such a study could provide useful information for future gTLD applicants. The RySG agrees.

We do not agree, however, that this should be a prerequisite to future rounds. Application decisions are not necessarily based on such data. What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

RySG comment:

The RySG reiterates our 2017 comment, with the strong restatement that this study should not be a prerequisite to future rounds. This study can only

determine if a registry's business model was successful so far at building trust amongst the surveyed population - it cannot preemptively gauge how much trust a specific business model will have in the future (particularly unless the specific target market is surveyed) and will not impact future applications. Furthermore, statements like "This information could inform future policy-making on the terms and conditions that should apply for all new gTLD applicants" imply that the CCT-RT believes new gTLD applicants are one-size fits all, with the same target market and drivers. This erroneous perception is pervasive throughout this Final Report and is a fatal flaw in its value as a set of recommendations.

**Chapter VIII. Consumer Trust**

**Recommendation 12:**

**Create incentives and/or eliminate current disincentives that encourage gTLD registries to meet user expectations regarding: (1) the relationship of content of a gTLD to its name; (2) restrictions as to who can register a domain name in certain gTLDs based upon implied messages of trust conveyed by the name of its gTLDs (particularly in sensitive or regulated industries) and (3) the safety and security of users’ personal and sensitive information (including health and financial information). These incentives could relate to applicants who choose to make Public Interest Commitments in their applications that relate to these expectations. TLD applicants for any subsequent rounds should be made aware of these public expectations by inserting information about the results of the surveys in an updated Applicant Guidebook.**

**Rationale/related findings:** The Nielsen surveys indicate certain expectations on the part of the public. They indicated the public believes that websites have different extensions to “properly identify the purpose or owner or to give an indication of content or function.”<sup>280</sup> The majority of those surveyed expect 1) a connection between the name of a gTLD and the websites associated with that gTLD and 2) a consistency between the meaning of the domain name and its actual use. The Nielsen surveys also indicate that the public expects restrictions on who can purchase domain names, expects that such restrictions will be enforced, and is concerned about the security of their personal and sensitive information. Hence, the Nielsen surveys indicated a positive relationship between registration restrictions and trustworthiness of a domain.

However, in practice, non-brand gTLDs with registration restrictions are extremely rare. Although the review team did not have any specific data sources to explain the general trend away from restricted TLDs, discussions with registries have indicated that the following factors discourage restricted business models:

- ICANN charges each TLD an up-front application fee of \$185,000 and an annual fee of \$25,000 regardless of the number of registrations within the gTLD. These fixed costs mean that smaller TLDs pay a much larger share of total revenue to ICANN than larger TLDs.
- The process of verifying compliance with restrictions may qualify as a “Registry Service”, which requires additional approval from ICANN and possibly additional fees to evaluate the service through ICANN’s Registry Service Evaluation Process (RSEP).
- Registration restrictions reduce the addressable market for the registry operator while increasing costs and adding friction to the registration process. Hence, profit-making registry operators generally tend to shy away from such restrictions. This is mirrored in legacy gTLDs and ccTLDs where many TLDs that initially operated with restrictions have subsequently removed or relaxed them, as with .pro, .travel, .fr and .ie.

Because consumer end-users expect restrictions, and the current market is largely not delivering restricted TLDs, the review team believes that future introductions of new gTLDs should consider examining whether it is possible to reduce existing disincentives to impose restrictions, or even to explicitly incentivize the adoption of restricted models by registry operators.

The fact that so few restricted TLDs exist despite these consumer expectations may also affect consumer trust in new gTLDs. As discussed later in this report in the section on Consumer Trust, consumers are generally less willing to share sensitive information to websites hosted on new gTLDs. Encouraging the protection of user data and/or registration restrictions on TLDs related to sensitive data sets (e.g. namespaces related to medical or financial data) may help address the existing gap in consumer trust.

**Details:** In addition to benefits in terms of trust, registration restrictions may also impact competition. Therefore, consideration should be given to both the potential benefits and drawbacks of registration restrictions.

**Success measures:** Measures of success for these recommendations would include improved public trust and visitation of new gTLDs and reduced fears regarding the misuse of users’ personal and sensitive information. They would also include an assessment of

**To**  
New gTLD Subsequent  
Procedures PDP  
Working Group

**Priority level**  
Prerequisite  
(incentives could be  
implemented as part of  
application process)



whether registration restrictions have had a negative impact on competition.		
--	--	--

RySG comment 2017: The nature of incentives isn't stated and therefore cannot yet be considered for support. Further, we do not support (1) and (2) as requirements—this in effect could be a form of content restriction, something the community, appropriately, is foursquare opposed to. (The Nielsen study may not have provided granularity to assess, for example, the possibility of a carpet cleaning service using the term Rug.Doctor, a perfectly legitimate use of the gTLD.) Creativity, without violating law, is a long-held hallmark of Internet naming and content and should not attempt to be curtailed.

We recommend the removal of (1) and (2).

The RySG supports (3).

As a prerequisite, what is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

RySG comment:

The RySG reiterates its 2017 comments. While the RySG recognizes the potential value of additional research on the benefits of registration restrictions, it strongly cautions the CCT-RT and the Board against using that sort of study to regulate business plans and content through forcing one model on all registry operators or otherwise inappropriately influencing competition within the domain name industry by incentivizing certain gTLD models and disadvantaging others.

Members of the RySG who operate or represent the operators of Verified TLDs maintain that registration restrictions are appropriate for gTLDs that operate in sensitive or regulated sectors. Registration restrictions add complexity and cost to business operations. While this is a burden the Registry Operator has voluntarily taken on, this comment should not be taken as a statement that individual operators of verified or restricted gTLDs should not be able to individually request reductions in their ICANN registry fees to account for those higher costs.

**Chapter VIII. Consumer Trust**

<p><b>Recommendation 13:</b>  <b>ICANN should collect data in conjunction with its related data-collection activities on the impact of restrictions on who can buy domains within certain new gTLDs (registration restrictions) to help regularly determine and report:</b></p> <ol style="list-style-type: none"> <li><b>(1). Whether consumers and registrants are aware that certain new gTLDs have registration restrictions;</b></li> <li><b>(2). Compare consumer trust levels between new gTLDs with varying degrees of registration restrictions;</b></li> <li><b>(3). Determine whether the lower abuse rates associated with gTLDs that impose stricter registration policies identified in the “Statistical Analysis of DNS Abuse in gTLDs” study continue to be present within new gTLDs that impose registration restrictions as compared with new gTLDs that do not;</b></li> <li><b>(4). Assess the costs and benefits of registration restrictions to contracted parties and the public (to include impacts on competition and consumer choice); and</b></li> <li><b>(5). Determine whether and how such registration restrictions are enforced or challenged.</b></li> </ol>		
<p><b>Rationale/related findings:</b> The ICANN Consumer Research and Registrant surveys indicate that the public expects certain restrictions about who can purchase domain names and trusts that these restrictions will be enforced. The survey results also indicated that the presence of such restrictions contributed to consumer trust. However, it would be useful for future review teams and those developing future policy to have more data on how aware the public is of registration restrictions and the impact of registration restrictions on consumer trust. In addition, the “Statistical Analysis of DNS Abuse in gTLDs” study indicated that DNS SecurityAbuse levels correlate with strict registration policies, with bad actors preferring register with no registration restrictions.<sup>284</sup> It is also important to obtain information on the costs of registration restrictions on the relevant parties so that benefits (in terms of increased trust and decreased DNS abuse) can be weighed against costs (including increased resources needed to implement such restrictions and financial costs) and any restrictions on competition. Future PDPs and review teams can use this data to inform future policy decisions regarding new gTLDs, especially as they relate to the issue of whether restrictions should be encouraged or included within the standard provisions included in ICANN new gTLD contracts.</p> <p><b>Details:</b> ICANN should explore how to incorporate this data collection as part of its existing data collection initiatives, including but not limited to the Domain Abuse Activity Reporting System and the gTLD Marketplace Health Initiative, as well as future ICANN initiatives related to measuring DNS abuse, and the health of the DNS and the DNS marketplace.<sup>285</sup> Moreover, ICANN may also explore how to incorporate this data collection through the activities and reporting of ICANN Contractual Compliance, including, but not limited to, its audit functions. Collecting this data would inform future review teams about the impact of registration restrictions and whether and how they can best be utilized for gTLDs, particularly those gTLDs that fall within sensitive or highly-regulated market sectors.</p> <p><b>Success measures:</b> This recommendation will be considered successful if it generates data that provides guidance for future review teams and policy development processes on the topic of registration restrictions, particular if the data indicates under what circumstances the benefits of registration restrictions to the public (which may include decreased levels of DNS abuse) outweigh possible costs to contracted parties or possible impacts on competition.</p>	<p><b>To</b>  ICANN organization</p>	<p><b>Priority level</b>  Low</p>
<p><b>RySG comment:</b>  See our comments to Recommendation 12. We additionally note that the RySG remains firmly opposed to using the Compliance audit function (which is designed to assess compliance with our contracts) to gain confidential business information. If ICANN desires this information, it can obtain it through independent research or through requests for voluntary information.</p>		

**Chapter IX. Safeguards**

**Recommendation 14:**

**Consider directing ICANN organization, in its discussions with registries, to negotiate amendments to existing Registry Agreements, or in consideration of new Registry Agreements associated with subsequent rounds of new gTLDs, to include provisions in the agreements to provide incentives, including financial incentives for registries, especially open registries, to adopt proactive anti-abuse measures.**

**Rationale/related findings:** ICANN is committed to maintaining “the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet.” The new gTLD safeguards alone do not prevent DNS Security abuse in the DNS and have consequently failed to meet their intended goal in preventing the abuse phenomenon from spreading to new gTLDs. The review team’s analysis and the DNS Abuse Study indicate that abuse rates are associated with registration restrictions imposed on registrants and registration prices (i.e., abuse rates tend to go down with increased registration restrictions and high domain name prices). Some registries are inherently designed to have strict registration policies and/or high prices. However, a free, open, and accessible Internet will invariably include registries with open registration policies and low prices that must adopt other measures to prevent DNS Security Abuse. Registries that do not impose registration eligibility restrictions can nonetheless reduce technical DNS Security Abuse through proactive means, such as identifying repeat offenders, monitoring suspicious registrations, and actively detecting abuse instead of merely waiting for complaints to be filed. Therefore, ICANN should incentivize and reward operators that adopt and implement proactive anti-abuse measures identified by the community as effective for reducing DNS Security Abuse. Operators that have already adopted such measures, prior to the creation of an incentive program, should be rewarded as well.

**Details:** The ICANN Board should consider urging ICANN organization to negotiate with new and legacy gTLD registries and registrars to include in the registry agreements fee discounts for registry operators with open registration policies and who implement proactive measures to prevent DNS Security Abuse in their zone. ICANN should verify compliance with incentive programs to ensure bad actors are not receiving incentives despite acting in bad faith. The adoption of proactive anti-abuse measures in exchange for incentives should not form the basis for shifting liability for underlying abuse incidents to the registry operator.

**Success measures:** More registries and registrars, even those with open registration policies, adopting proactive anti-abuse measures that result in measurable decreases in the overall rates of DNS Security Abuse in their zones.

**To**  
The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, and the Subsequent Procedures PDP WG.

**Priority level**  
High

Jan 2018 RySG comment: The RySG supports recognizing and supporting the many ROs that take steps to discourage abuse, but opposes amending the RA as recommended, to mandate or incentivize ‘proactive’ anti-abuse measures.

This recommendation raises a number of questions, including what types of anti-abuse measures would qualify for what types of incentives. Without a clear, agreed-upon definition of abuse, this could be challenging. Coming to such a definition will, as the RySG knows from experience, be a long, complex process; following which, the parties must negotiate the relevant registry agreement amendments.

Providing financial incentives to registries through a reduction in ICANN fees could have the unintended consequence of higher abuse rates from the increased

availability of cheaper domains. While good actors will ensure proper countermeasures are in place when engaging in lower price selling, there is no guarantee that existing bad actors would take advantage of such incentives, or live up to their obligations under any such program, resulting in no net improvement to the current situation. Such incentives could also backfire and serve as a disincentive against registries that utilize “non-traditional” or innovative business models, such as restricted namespaces with higher operational costs and, as such, higher registration prices.

Tracking the effectiveness of anti-abuse measures to determine whether the registry continues to qualify for the incentive would create a significant operational burden on ICANN, which could then increase operational costs.

If this recommendation is accepted, the RySG notes that only offering incentives to completely open TLDs doesn’t go far enough to recognize the valuable protections strict registration policies or high prices or other mechanisms bring to the DNS. Any incentives ICANN might propose should include ALL actions taken by ROs to protect the TLD from technical abuse without a presumption or preference for a particular business model.

With particular reference to the suggested inclusion of **proactive** abuse mitigation within the Registry Agreement, it is noted that such contractual obligations may have the potential to create an increased risk of legal liability for the registry operator. Should contracted parties accept a financial benefit in return for undertaking **proactive** abuse mitigation, a substantial risk occurs that should they fall short in this task (fail to discover (an) abuse(s), which may cause harm or loss (e.g. phishing, malware dissemination, botnet/C&C)). A registry operator, having accepted a specifically preventative responsibility in their RA, would be at a distinct legal disadvantage if attempting to disclaim liability, were they joined to any action arising out of such an abuse.

RySG comment:

The RySG reiterates its January 2018 comment. Furthermore, we note that registries have to weigh much more than just “is abuse happening.” The decision matrix is complex and there are legal, business, and political outcomes to consider. This recommendation is extremely short-sighted and only looks at the issue of DNS abuse one-dimensionally.

Chapter IX. Safeguards

**Recommendation 15:**

ICANN Org should, in its discussions with registrars and registries, negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars or registries for DNS Security Abuse. With a view to implementing this recommendation as early as possible, and provided this can be done, then this could be brought into effect by a contractual amendment through the bilateral review of the Agreements. In particular, ICANN should establish thresholds of abuse at which compliance inquiries are automatically triggered, with a higher threshold at which registrars and registries are presumed to be in default of their agreements. If the community determines that ICANN org itself is ill-suited or unable to enforce such provisions, a DNS Abuse Dispute Resolution Policy (DADRP) should be considered as an additional means to enforce policies and deter against DNS Security Abuse. Furthermore, defining and identifying DNS Security Abuse is inherently complex and would benefit from analysis by the community, and thus we specifically recommend that the ICANN Board prioritize and support community work in this area to enhance safeguards and trust due to the negative impact of DNS Security Abuse on consumers and other users of the Internet.

**Rationale/related findings:** Published research, cybersecurity analysis, and DNS Security Abuse monitoring tools highlight concentrated, systemic DNS Security Abuse for which there are no adequate, actionable remedies. The CCT-RT is of the view that the existing powers of ICANN Compliance are too weak in their present form to be as effective as they need to be in abating such DNS Technical Abuse, and ICANN Compliance needs clear authority to address systematic abuse effectively. Whilst abuse can be due, in part, to negligent parties, one of the specific areas of concern identified nearly a decade ago by the community prior to the launch of the New gTLD Program was how to ensure that “bad actors” do not run registries[1]. The anti-abuse safeguards put in place as part of the new gTLD program do not address this problem. Examples from the DNS Abuse Study of new gTLDs registrars with more than 10% of their domain names blacklisted as well as registries, according to Spamhaus for example are .science (51%), .stream (47%), .study (33%), .download (20%), .click (18%), .top (17%), .gdh (16%), .trade (15%), .review (13%), and .accountant (12%). Current policies focus on individual abuse complaints and an ineffective duty to investigate. Such abuse as has been identified by the DNS Abuse Study[2] concentrated in particular in certain registries and registrars and despite such identification it appears that ICANN Compliance are unable to remedy the situation whereby ICANN may suspend registrars and registry operators found to be associated with unabated, abnormal and extremely high rates of DNS Security Abuse. In this paradigm, certain registrars and registry operators associated with extremely high rates of DNS Security Abuse have continued to operate and face little incentive to prevent such malicious activity. Moreover, there currently exist few enforcement mechanisms to prevent systemic domain name abuse associated with resellers. Systemic use of particular registrars and registries for DNS Security Abuse threatens the security and stability of the DNS, the universal acceptance of TLDs, and consumer trust. Consequently, the imposition of contractual requirements and effective means to enforce them are necessary to remedy this unacceptable phenomenon.

**Details:** The ICANN Board should direct ICANN Org to negotiate amendments to the Registrar Accreditation Agreement and Registry Agreement provisions aimed at preventing DNS Security Abuse. Such language should impose upon registries and registrars, and through downstream contract requirements their affiliated entities such as resellers, a duty to prevent wide-scale DNS Security Abuse and implement specific measures to reduce malicious conduct whereby ICANN may suspend registrars and registry operators found to be associated with unabated, abnormal and extremely high rates of DNS Security Abuse. It is important for ICANN Org to gather relevant data, conduct analysis, and act on actionable information. Accordingly, ICANN should initiate an investigation into a contracted party’s director indirect (such as through a reseller) involvement with systemic DNS Security Abuse. ICANN should make use of well-regarded abuse/black lists and establish an initial threshold at which compliance inquiries are automatically generated. We suggest that this initial threshold should be 3% of registrations or 30 total registrations, whichever is higher. Further, ICANN should establish a subsequent threshold at which a contracted party is presumed to be in breach of its agreement. We suggest this subsequent threshold should be 10% of registrations or 100 total registrations, whichever is higher.

**To**  
The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG

**Priority level**  
Prerequisite (provisions to address systemic DNS Security Abuse should be included in the baseline contract for any future new gTLDs)

Upon making a finding and contacting the contracted party, such findings may be rebutted upon sufficient proof that the findings were materially inaccurate or that the TLD operator is actively mitigating the identified DNS Security Abuse. The following factors may be taken into account when making a determination: whether the registrar or registry operator 1) engages in proactive anti-abuse measures to prevent DNS Security Abuse, 2) was itself a victim in the relevant instance, 3) has since taken necessary and appropriate actions to stop the abuse and prevent future systemic use of its services for DNS Security Abuse.

It is imperative that ICANN Org be empowered to deal with systemic DNS Security Abuse. However, in addition, a specific DADRP should be considered to the extent the community concludes that ICANN Compliance may be unable or ill-suited to deal with certain situations related to such abuse. Where proper, a DADRP could serve as a significant deterrent and help prevent or minimize such high levels of DNS abuse. Analogous to the Trademark PDDRP, this tool would empower the community to address systemic DNS Security Abuse, which plagues the security and stability of Internet infrastructure and undermines safeguards aimed at ensuring consumer trust. Such a procedure would apply if ICANN Compliance were not the right body to resolve a complaint related to DNS Security Abuse, is ill-suited or unable to do so and the registry operators or registrars are identified as having excessive levels of abuse. It may be useful for Compliance to be able to refer a case to the DADRP. The Community should determine the conditions under which a complainant can invoke a DADRP.

**Success measures:** 1) Contractual language is adopted which empowers ICANN to investigate and engage in enforcement actions against registries and registrars associated with systemic DNS Security Abuse such that there are no contracted parties serving as enablers of systemic DNS Security Abuse for which ICANN cannot bring an enforcement action. 2) A DADRP is created if there is an area of DNS Security Abuse that ICANN Org is unable to address 3) There exist no gTLD or registrar with systemic high levels of DNS Security Abuse (>3%). 4) The total volume of DNS Security Abuse decreases.

Jan 2018 RySG comment: *The RySG strongly opposes this Recommendation.* Specification 11 of the new gTLD Registry Agreement states that new gTLD Registry Operators may only use ICANN-accredited registrars. To the extent that this recommendation pertains to new gTLD registries, that would put ICANN org in the position of endeavoring to prevent the use of registrars that it accredits, which will likely violate a registry's equal access obligations. This recommendation attempts to force gTLD registries to do what ICANN cannot: indirectly control resellers. ICANN must not shift its Contractual Compliance responsibilities to ROs, which this Recommendation effectively seeks to do.

Introducing additional policies or provisions to promote behavior beyond what is already mandated in registry and registrar agreements suggests that current enforcement of existing policies should be prioritized. If bad actors are identified, action should be taken by ICANN to discipline or de-accredit those actors, as occurs with other breaches of ICANN's agreements.

Furthermore, the RySG opposes any scheme in which a contracted party is deemed guilty until it proves its innocence. ICANN has shown a great willingness through its DAAR program to consider third-party ("3P") abuse monitoring services to be "multiple verifiable reliable sources" when these 3P sources have not been vetted or reviewed by the community. ICANN must not suspend a contracted party and potentially destroy its reputation, based solely on 3P sources.\*\* This is particularly true for ROs that are, or are affiliates of, publicly traded companies. ICANN's willingness to do – especially where ICANN Org has repeatedly stated its refusal to accept any liability for this potential damage – is irresponsible and inconsistent with ICANN's bylaws. The RySG strongly objects to placing the business and reputations of contracted parties at the whim, error, or (mis)interpretation of 3Ps.

The CCT-RT must take into account that each of the 3P sources ICANN uses for DAAR has its own, independent (i.e. not controlled by any standards organization)

definition of abuse. So does each contracted party. No community-defined process exists to classify a 3P abuse report of conduct that violates the 3P's "abuse" definition, but does not violate the relevant contracted party's "abuse" definition. ICANN must openly and transparently identify how it will address these and other concerns before it releases and relies upon DAAR.

AND also from the Jan 2018 RySG comment:

The RySG strongly disagrees with the proposal to create a DNS Abuse Dispute Resolution Procedure (DADRP) and supports the rationale of the Minority Statement on this Recommendation. We have concerns about committing registry operators to be bound to a new DRP when our contracts with ICANN already require that we take measures to mitigate abuse. The DADRP proposal is premised upon the false assumption that registries are directly responsible for abuse within their TLDs; however, registries generally have no direct relationship with registrants and little control over how domains are used once registered. As is acknowledged in the CCT-RTs own report, registry-level safeguards have proven ineffective at reducing DNS abuse. Further, registries with the concentrations of abuse contemplated within the section are a small few, and are readily identifiable without relying upon a third party trigger. Improvements should be made to the existing compliance function rather than relying upon a whole new procedure to handle enforcement in a very narrow subset of cases, where there is no evidence that such a procedure is necessary or would be effective in achieving its intended aim. The alternative of creating the DADRP creates uncertainty and potential operational burden for registries without clear benefit. We also refer again to the over reliance on 'blacklists' in this context. Whereas it can be accepted that data sourced from blacklists are useful as red flag indicators, the actual data remain formally unverified, and underlying evidence remains largely unavailable to any affected party. Its with much dismay that we note the continued justification for the use of such sources based on nebulous concepts such as 'widespread use' and 'reputation', rather than on actual sound verification of the underlying data. It has been publicly accepted by ICANN Compliance (ICANN 60 DNS Abuse Reporting & Mitigation Session) that the use of such blacklists alone at the aggregate level, would not be deemed sufficient to ground contractual enforcement, and as such it is inappropriate to suggest that the same sources are somehow suitable to similarly ground a DRP. Developing this DADRP would require a significant outlay of time, energy and resources from the community – especially considering that there is no clear definition of "abuse" – with little obvious benefit or return on that effort. In addition, this recommendation raises the possibility of involving a third party in the interpretation of our contracts, which is a proposition that the RySG cannot support. Any such step would require a GNSO PDP, at a minimum.

RySG comment:

The RySG reiterates its January 2018 comments.

## Chapter IX. Safeguards

### Recommendation 16:

**Further study the relationship between specific registry operators, registrars, and DNS Security Abuse by commissioning ongoing data collection, including but not limited to, the ICANN Domain Abuse Activity Reporting (DAAR) initiative. For transparency purposes, this information should be regularly published, ideally quarterly and no less than annually, in order to enable identification of registries and registrars that require greater scrutiny, investigation, and potential enforcement action by the ICANN organization. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remedy problems identified, and define future ongoing data collection.**

**Rationale/related findings:** Comprehensive DNS Security Abuse data collection and analysis is necessary for studying the efficacy of safeguards put in place to protect against malicious abuse issues associated with the expansion of the DNS. Furthermore, progress and trends can be identified by repeating studies over time. The DNS Abuse Study commissioned by the CCT Review Team identified extremely high rates of abuse associated with specific registries and registrars as well as registration features, such as bulk registrations, which appear to enable abuse. Moreover, the Study concluded that registration restrictions correlate with abuse, which indicates that there are many factors to consider and analyze in order to extrapolate cross-TLD abuse trends for specific registry operators and registrars. The DNS Abuse Study highlighted certain behaviors that are diametrically opposed to encouraging consumer trust in the DNS. Certain registries and registrars appear to either positively encourage or at the very least willfully ignore DNS Security Abuse. Such behavior needs to be identified and acted upon quickly by the ICANN organization as determined by the facts and evidence presented. The DNS Abuse Study, which provided a benchmark of DNS Security Abuse since the onset of the New gTLD Program, should be followed up with regular studies so that the community is provided current, actionable data on a regular basis to inform policy decisions.

**Details:** The additional studies need to be of an ongoing nature, collecting relevant data concerning DNS Security Abuse at both the registrar and registry level. The data should be regularly published, thereby enabling the Community and the ICANN organization in particular to identify registries and registrars that need to come under greater compliance scrutiny and thereby have such behavior eradicated.

**Success measures:** Comprehensive, up-to-date technical DNS Security Abuse data is readily available to the ICANN Community to promptly identify problems, craft data-driven policy solutions, and measure the efficacy of implemented safeguards and ongoing initiatives. Furthermore, the next CCT Review Team will have a rich dataset on DNS abuse from which to measure safeguard efficacy.

**To**  
The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, and the Subsequent Procedures PDP WG, SSR2 Review Team.

**Priority level**  
High

Jan 2018 RySG comment: The RysG supports the recommendation that ICANN conduct ongoing research on DNS abuse, but cautions against using the DNS Abuse Study to come to any conclusions and strongly opposes the use and publication of data from DAAR.

While the RySG respects the intent and efforts of the researchers who conducted the DNS Abuse Study, the RySG believes the study is flawed and it should not be the basis for any decisions. These flaws include: The study is self-referencing and in many cases only references prior work by the same authors (see the Reference list in the study where the authors repeatedly quote themselves). The study makes conclusions for which it provided no data or analysis in the text (despite no data about price, and only mentioning price twice as a sidenote, the study concludes that lower prices might be linked to abuse). The study circularly relies on the statements of the tools it chose to use, (i.e. citation to Spamhaus itself for its assertion that Spamhaus is a “near zero false positive list”).

The RySG is not opposed to ongoing anonymized data collection to learn more about abusive behaviors but strongly recommends that the researchers chosen be



required to provide clear reports that link every conclusion to a specific data point and analysis. Even though the RySG does note that the report contains some positive, and well-researched findings based on data (such as the findings that most new gTLDs are not havens for abuse or malware), the quality of the study is lacking enough that care should be taken when interpreting all of the results.

Furthermore, as mentioned previously, ICANN has created DAAR behind closed doors, with no community consultation, and determined which 3Ps data feeds it will rely on, without input from the community. ICANN has apparently, in determining how “trusted” these 3Ps are, relied on the cost-benefit-risk analysis of corporate IT departments that pay for filtering rather than the needs and interests and concerns of the community, and particularly contracted parties. Although there is much benefit to be had in establishing reliable tools for the measurement and mitigation of abuse, which it is assumed is the ultimate aspiration for the DAAR project, any current reliance on DAAR is exceptionally premature. The CCT-RT should not recommend use of DAAR to monitor or police contracted parties, until the community has had a chance to discuss and debate the impact, benefits and risks to the various constituencies. In particular, the CCT-RT should not recommend that ICANN publish the data from DAAR until there is a mechanism in place for addressing community concerns that does not jeopardize the reputation or business of the RO without a fair and impartial investigation, and ICANN acknowledges its potential liability for reliance on DAAR.

**RySG comment:**

The RySG reiterates its 2018 comment. Furthermore, the RySG notes that the extensive public-relations campaign that ICANN Org is conducting for DAAR and its data is not a substitute for actual community consultation with the parties that will be affected by its use.

## Chapter IX. Safeguards

### Recommendation 17:

**ICANN should collect data about and publicize the chain of parties responsible for gTLD domain name registrations.**

**Rationale/related findings:** At present, there is no consistent mechanism for determining all of the ICANN-contracted and non-contracted operators associated with a gTLD domain name registration. WHOIS records often do not distinguish between registrars and resellers. The DNS Abuse Study, for example, was unable to discern resellers from registrars to determine the degree to which DNS Security Abuse rates may be driven by specific-resellers, which in turn affects overall levels of DNS Security abuse. This data should be available to enhance data-driven determinations necessary for recommendations proposed by this and future CCT Review Teams, supplement New gTLD Program safeguards, and improve ICANN Contractual Compliance determinations.

**Details:** WHOIS information is an important source of data for DNS Security Abuse analysis. Safeguards, such as the Thick WHOIS requirements, do not mandate that resellers be listed in WHOIS records. Consequently, the full chain of parties to a registration transaction is not readily discernible. Without such information, it is difficult to determine the extent to which DNS Security Abuse is correlated to individual resellers rather than registrars. For example, with such data hidden, it would be possible for a reseller associated with extremely high levels of abuse to remain in operation under a registrar with relatively normal levels of DNS Security Abuse. This would, in effect, permit systemic DNS Security Abuse by a non-contracted party. Although the reseller is theoretically bound by flow-down contract requirements, in practice this systemic DNS Security Abuse often remains difficult to attribute and tends to go unabated. Whereas, collecting and publicizing such information would enable end-users to readily determine the registry, registrar, and reseller associated with malicious domain name registrations. This would allow for more granular DNS abuse analysis as well as transparency for Internet users, thereby enhancing Community accountability efforts and Contractual Compliance enforcement.

**Success measures:** It is possible for anyone to readily determine the reseller associated with any gTLD registration.

**To**  
The ICANN Board, the GNSO Expedited PDP, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, the Subsequent Procedures PDP WG, SSAC

**Priority level**  
High

#### RySG comment:

The RySG notes that the CCT-RT needs to define “reseller” before it can suggest that ICANN should track them all. Every private sale of a domain name is a “resale” so it’s important for the community and the Board to understand exactly what it’s been asked to approve here. At a minimum this would require a new PDP.

**Chapter IX. Safeguards**

**Recommendation 18:**

In order for the upcoming WHOIS Review Team to determine whether additional steps are needed to improve WHOIS accuracy, and whether to proceed with the “identity” phase of the Accuracy Reporting System (ARS) project, ICANN should gather data to assess whether a significant percentage of WHOIS-related complaints applicable to new gTLDs relate to the accuracy of the identity of the registrant. This should include analysis of WHOIS accuracy complaints received by ICANN Contractual Compliance to identify the subject matter of the complaints (e.g., complaints about syntax, operability, or identity). The volume of these complaints between legacy gTLDs and new gTLDs should also be compared. ICANN should also identify other potential data sources of WHOIS complaints beyond those that are contractually required (including, but not limited to, complaints received directly by registrars, registries, ISPs, etc.) and attempt to obtain anonymized data from these sources.

Future CCT Review Teams may then also use these data.

**Rationale/related findings:** WHOIS-related complaints are the largest category of complaints received by ICANN Contractual Compliance for registrars. However, it is unclear what aspect of WHOIS accuracy forms the basis of these complaints, or if the introduction of new gTLDs has had any effect on the accuracy of WHOIS data. Phase 1 of ICANN’s ARS project analyzes the syntactic accuracy of WHOIS contact information and Phase 2 assesses the operability of the contact data in the WHOIS record. But there is currently no plan to proceed with Phase 3 of the ARS project: identity validation (is the contacted individual responsible for the domain?).

**Success measures:** Availability of data that shows the breakdown of WHOIS accuracy complaints by subject matter (syntax, operability or identity). Availability of data that allows comparison between legacy gTLDs and new gTLDs. Availability of data to inform the upcoming WHOIS Review Team on where further work is needed to improve WHOIS accuracy.

**To**  
ICANN organization to gather required data, and to provide data to relevant review teams to consider the results and, if warranted, to assess feasibility and desirability of moving to identity validation phase of WHOIS ARS project.

**Priority level**  
Medium

RySG comment:

In light of GDPR, the EPDP, and the changing nature of Whois/RDDS, the RySG strongly recommends this recommendation be at least postponed, and possibly withdrawn, pending the outcome of the data privacy work. If the recommendation is not withdrawn the CCT-RT should first consider: what is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

## Chapter IX. Safeguards

### Recommendation 19:

The next CCT Review Team should review the "Framework for Registry Operator to Respond to Security Threats" and assess whether the framework is a sufficiently clear and effective mechanism to mitigate abuse by providing for systemic and specified actions in response to security threats.

**Rationale/related findings:** It is not clear whether the intended goal of the "security checks" safeguard to strengthen efforts to fight DNS abuse has been met. The Community will be better positioned to evaluate the effectiveness of this safeguard once the "Framework for Registry Operator to Respond to Security Threats" is in place for a sufficient period of time to provide more specific information.

**Details:** It is not clear whether the intended goal of the "security checks" safeguard has been met. With the voluntary framework in place as of October 2017, the Community will be better positioned to evaluate the effectiveness of this safeguard.

**Success measures:** An evaluation of the "Framework for Registry Operator to Respond to Security Threats."

**To**  
Future CCT Review  
Teams

**Priority level**  
Medium

### RySG comment:

The Framework for Registry Operator to Respond to Security Threats was the result of voluntary, good faith discussions by registry operators and is not an ICANN Consensus policy. Future CCT Review Teams should bear in mind that the Framework itself is a voluntary and non-binding document, and as such, any evaluations of the Framework should seek to engage Registry Operators on a voluntary basis. ICANN's Compliance department should not be leveraged to gather data about the Framework. Further, future Review Teams should exercise caution in extrapolating conclusions that apply to all gTLD registries from such a review.

**Chapter IX. Safeguards**

**Recommendation 20:**

Assess whether mechanisms to report and handle complaints have led to more focused efforts to combat abuse by determining: (1) the volume of reports of illegal conduct in connection with the use of the TLD that registries receive from governmental and quasi-governmental agencies; (2) the volume of inquires that registries receive from the public related to malicious conduct in the TLD; (3) whether more efforts are needed to publicize contact points to report complaints that involve abuse or illegal behavior within a TLD; and (4) what actions registries have taken to respond to complaints of illegal or malicious conduct in connection with the use of the TLD. Such efforts could include surveys, focus groups, or Community discussions. If these methods prove ineffective, consideration could be given to amending future standard Registry Agreements to require registries to more prominently disclose their abuse points of contact and provide more granular information to ICANN. Once this information is gathered, future review teams should consider recommendations for appropriate follow up measures.

**Rationale/related findings:**

The Consumer Research and Registrant surveys conducted by Nielsen have shown significant consumer concern related to abuse, which may undermine confidence and trust in the DNS. The broad strategic response should be to ensure that there are sufficiently effective mechanisms to report complaints that can be measured and assessed, and hence develop the capacity to manage and mitigate the causes of these complaints.

There is concern from the Community that abuse data is not reported consistently to registries. Other concerns relate to ICANN’s own reporting of the complaints it receives. In particular, those concerns focus on the lack of granularity regarding the subject matter of the complaints and lack of information regarding the response to abuse complaints. Generally speaking, detailed information regarding the subject matter of complaints and responses to those complaints is sparingly captured and shared, missing, or unknown.

Although the safeguards regarding making and handling complaints have been implemented, in light of the concerns noted above, it is unclear: (1) whether either law enforcement or the public is sufficiently aware that these complaint mechanisms exist; (2) how frequently these channels are used by the public and law enforcement to notify registries of illegal or abusive behavior; and (3) what impact these safeguards have had on their intended goal of mitigating DNS abuse. Hence, the review team’s recommendations relate to improved data gathering to inform future efforts to combat abuse within gTLDs.

**Success measures:**

- More information is gathered to assess whether current complaint reporting mechanisms are effective, and that this information informs policy efforts involving amendment of standard Registry agreements.
- ICANN Contractual Compliance routinely records and makes available information about complaints by categories filed from registry and registrars, including responses to reports of abuse to original reporters.

**To**  
ICANN organization  
and future CCT Review  
Teams

**Priority level**  
Medium

RySG comment:

As the review team notes in the Report, the contractual requirement in the RA regarding this safeguard is narrowly defined to the following: “Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD.” As such, part (2) of the Recommendation 20 is inappropriate as it expands beyond Registry Operators’ contractual obligations, especially given the fact that merely measuring the volume of inquiries does not necessarily provide a clear

picture of how much malicious conduct is actually taking place in a given gTLD. Abuse contacts, especially when published in an easily accessible place, receive high volumes of spam and other insignificant emails that do not contain specific inquiries or complaints about demonstrable malicious conduct.

**Chapter IX. Safeguards**

**Recommendation 21:**

**Include more detailed information on the subject matter of complaints in ICANN publicly available Contractual Compliance reports. Specifically, more precise data on the subject matter of complaints should be included, particularly: (1) the class/type of abuse; (2) the gTLD that is target of the abuse; (3) the safeguard that is at risk; (4) an indication of whether complaints relate to the protection of sensitive health or financial information; (5) what type of contractual breach is being complained of; and (6) resolution status of the complaints, including action details. These details would assist future review teams in their assessment of these safeguards.**

**Rationale/related findings:**

(Note: A general recommendation for further transparency regarding the subject matter of complaints received by ICANN Contractual Compliance is set forth in [Chapter 5: Data-Driven Analysis: Recommendations for Additional Data Collection and Analysis.](#))

The lack of publicly available information about whether ICANN Contractual Compliance has received complaints related to the implemented Category 1 safeguards, and lack of a common framework to define sensitive information and identify what constitutes “reasonable and appropriate security measures” make it difficult to assess what impact this safeguard has had on mitigating risks to the public.

The results of the Consumer Research and Registrant Surveys by Nielsen indicate that new gTLDs are not trusted to the same extent as legacy gTLDs, and that the public is concerned about potential misuse of their personal information. Domains catering to interests in highly- regulated sectors such as health and finance are likely to collect more personal and sensitive information. So in that sense, trustworthiness of these domains is even more crucial. There is a further concern that complaints about illegal DNS activities may be under-reported.

Although ICANN has mandated certain safeguards applicable to all new gTLD domains in general and domains for highly-regulated strings in particular, there is scant evidentiary data that the contracted parties have implemented and are complying with these safeguards. The review team lack the evidence to definitively declare whether the defined and implemented safeguards have been effective in mitigating risks associated with domains in the overall new gTLD market, and those in highly-regulated markets in particular. Hence, it is desirable to gather sufficient information to understand whether the existing safeguards mitigate the risks assessed for the new gTLD domains, especially those associated with highly-regulated sectors, and whether there is adequate and effective enforcement. The recommendation therefore proposes that ICANN Contractual Compliance collect and provide reports on the abuse reported to registry and registrars with a granularity that allows identification of origin, type, form, and nature of abuse or alleged illegal use of the DNS.

The ICANN organization acknowledges that data on the several safeguards is not currently being collected in either the detail expected or at all. However, there are ongoing data collection activities and initiatives that may remedy this situation.

**Details:** This recommendation is tied to the previous one. Together they aim to address whether the New gTLD Program safeguards, the mechanisms developed to implement them, and the outcomes of those implementations allow a reviewer to draw a definitive conclusion on their effectiveness and fitness to purpose.

**Success measures:** ICANN Contractual Compliance publication of a formatted report on abuse reports received and adjudicated, including, at minimum, all of the specified types and categories noted above.

**To**  
ICANN organization

**Priority level**  
High

RySG comment:

The wording of this recommendation should be updated to reflect that it pertains specifically to sensitive and regulated gTLD strings. Additionally, the RySG wishes to note that the remit of ICANN's Compliance department is to monitor contracted parties' compliance with terms of their respective ICANN contracts (in the case of registries, the Registry Agreement). This recommendation should not provide ICANN Compliance with justification to require Registry Operators to provide data about activities that extend beyond their compliance with the terms and provisions of their individual Registry Agreements.



## Chapter IX. Safeguards

### Recommendation 22:

**Initiate engagement with relevant stakeholders to determine what best practices are being implemented to offer reasonable and appropriate security measures commensurate with the offering of services that involve the gathering of sensitive health and financial information. Such a discussion could include identifying what falls within the categories of “sensitive health and financial information,” and what metrics could be used to measure compliance with this safeguard.**

**Rationale/related findings:** The lack of publicly available information about whether ICANN Contractual Compliance has received complaints related to the implemented Category 1 safeguards, and lack of a common framework to define sensitive information, makes it difficult to assess what impact this safeguard has had on mitigating risks to the public. However, protection of sensitive information, particularly sensitive financial and health information, is a high priority for Internet users. As a result, this recommendation aims at improving both complaint data regarding these issues and encouraging communications about best practices on how to protect these sensitive categories of information.

**Success measures:** This recommendation would be successful if relevant stakeholders, including new gTLD registries and stakeholder groups representing the public interest, discuss what constitutes sensitive information and best practices regarding how to protect sensitive information. Such discussions could inform future policy in this area with a goal of increasing the public’s trust of new gTLDs.

**To**  
ICANN organization

**Priority level**  
High

### RySG comment:

This recommendation is overbroad and should be limited to sensitive and regulated TLD strings that have taken on an affirmative duty to protect the public in their PICs. The RySG are willing to have a discussion about we are doing with respect to sensitive information, but the CCT-RT is once again reminded that we do not collect sensitive information on websites we do not control.

**Chapter IX. Safeguards**

<p><b>Recommendation 23:</b>  <b>ICANN should gather data on new gTLDs operating in highly-regulated sectors to include the following elements:</b></p> <ul style="list-style-type: none"> <li>● <b>A survey to determine 1) the steps registry operators are taking to establish working relationships with relevant government or industry bodies, and 2) the volume of complaints received by registrants from government and regulatory bodies and their standard practices to respond to those complaints;</b></li> <li>● <b>A review of a sample of domain websites within the highly-regulated sector category to assess whether contact information to file complaints is sufficiently easy to find;</b></li> <li>● <b>An inquiry to ICANN Contractual Compliance and registrars/resellers of highly- regulated domains seeking sufficiently detailed information to determine the volume and the subject matter of complaints regarding domains in highly-regulated industries.</b></li> <li>● <b>An inquiry to registry operators to obtain data to compare rates of abuse between those highly-regulated gTLDs that have voluntarily agreed to verify and validate credentials to those highly-regulated gTLDs that have not.</b></li> <li>● <b>An audit to assess whether restrictions regarding possessing necessary credentials are being enforced by auditing registrars and resellers offering the highly-regulated TLDs (i.e., can an individual or entity without the proper credentials buy a highly- regulated domain?).</b></li> </ul> <p><b>To the extent that current ICANN data collection initiatives and Contractual Compliance audits could contribute to these efforts, the review team recommends that ICANN assess the most efficient way to proceed to avoid duplication of effort and leverage current work.</b></p>		
<p><b>Rationale/related findings:</b>  Although ICANN has implement certain safeguards applicable to domains operating in highly-regulated sectors, it is unclear whether and how contracted parties are complying with these safeguards. It is also not clear whether these safeguards have been effective in mitigating risks associated with domains in highly- regulated markets. The Nielsen consumer end-user survey results indicate that new gTLDs are not trusted to the same extent as legacy gTLDs and that the public is concerned about potential misuse of their sensitive information. Domains working in highly-regulated sectors such as health and finance may be more apt to collect this sensitive information, and hence the trustworthiness of these domains is even more crucial. Accordingly, it is important to understand whether the safeguards put into place to mitigate the risks associated with highly- regulated domains are being enforced and whether they are effective.</p> <p><b>Details:</b> ICANN is embarking on several data gathering initiatives that may shed light on some of these issues, including the Domain Abuse Activity Reporting Project, the gTLD Marketplace Health Index, and the Identifier Technology Health Indicators project.<sup>448</sup> Moreover, ICANN Contractual Compliance is expanding its audit functions to include additional examination of compliance with certain safeguards. Hence, consideration should be given to assessing whether ICANN’s ongoing data collection and Contractual Compliance initiatives could be leveraged to implement parts of this recommendation.</p> <p><b>Success measures:</b> This recommendation will be successful if additional data is generated to inform ongoing policy development processes regarding the effectiveness of ICANN contract provisions intended to safeguard the public, particularly as they relate to new gTLDs operating in highly-regulated sectors, and whether the current contractual safeguards sufficiently protect the public against the higher risks associated with these domains. In particular, it is vital to determine whether the current safeguard requiring that</p>	<p><b>To</b>  ICANN organization and Subsequent Procedures PDP Working Group</p>	<p><b>Priority level</b>  High</p>

registrants possess appropriate credentials for gTLDs operating in highly-regulated sectors is working as intended. Success in this regard would be to generate an assessment of complaints relating to this safeguard, including information on how this safeguard is enforced, among other factors, in order to determine its effectiveness.		
--	--	--

RySG comment:

Again, the RySG wishes to note that the remit of ICANN's Compliance department is to monitor contracted parties' compliance with terms of their respective ICANN contracts (in the case of registries, the Registry Agreement). This recommendation should not provide ICANN Compliance with justification to require Registry Operators to provide data about activities that extend beyond their compliance with the terms and provisions of their individual Registry Agreements. While certain RySG members acknowledge that gathering data regarding the operation of gTLDs in highly-regulated sectors would be useful, we urge that any data collection efforts should be voluntary.

## Chapter IX. Safeguards

### Recommendation 24:

1. Determine whether ICANN Contractual Compliance should report on a quarterly basis whether it has received complaints for a registry operator's failure to comply with either the safeguard related to gTLDs with inherent governmental functions or the safeguard related to cyberbullying.
2. Survey registries to determine 1) whether they receive complaints related to cyberbullying and misrepresenting a governmental affiliation, and 2) how they enforce these safeguards.

**Rationale/related findings:** The lack of information about whether ICANN Contractual Compliance or registries have received complaints related to these safeguards and lack of consequences for failure to comply with these safeguards make it difficult to assess their effectiveness in mitigating the risks they were intended to address. Gathering this information would assist future policy development processes by identifying whether the current safeguards are meeting their intended goal. (Note: A general recommendation for further transparency regarding the subject matter of complaints received by ICANN Contractual Compliance is set forth in [Chapter 5: Data-Driven Analysis: Recommendations for Additional Data Collection and Analysis](#).)

**Success measures:** These recommendations will be successful if they generate data that indicates the magnitude of complaints regarding cyberbullying and misrepresenting governmental affiliations and provide information regarding how registries enforce these safeguards.

**To**  
ICANN organization

**Priority level**  
Low

### RySG comment:

The RySG notes that the safeguards mentioned in Recommendation 24 pertain only to a small group of new gTLDs and as a matter of course, the RySG does not comment on issues related to specific gTLD registries. That said, however, we would like to point out that the report states, "It is not clear whether failure to comply with these safeguards has generated complaints," which presumes that such failures have occurred, despite providing no evidence to support that presumption.

**Chapter IX. Safeguards**

**Recommendation 25:**

**To the extent voluntary commitments are permitted in future gTLD application processes, all such commitments made by a gTLD applicant must state their intended goal and be submitted during the application process so that there is sufficient opportunity for Community review and time to meet the deadlines for Community and limited public interest objections. Furthermore, such requirements should apply to the extent that voluntary commitments may be made after delegation. Such voluntary commitments, including existing voluntary PICs, should be made accessible in an organized, searchable online database to enhance data-driven policy development, Community transparency, compliance, and awareness of variables relevant to DNS abuse trends.**

**Rationale/related findings:** The intended purpose of many existing voluntary commitments, through the form of voluntary PICs, is not readily discernible. This ambiguity stifles the Community's ability to evaluate effectiveness. Moreover, upon submission of a gTLD application, there is no mechanism in place for the Community to ensure that such commitments do not negatively impact the public interest and other aspects of the DNS. Consequently, it is important to the multistakeholder process that such voluntary commitment proposals be made available to the Community with adequate time for assessment and potential objections. Furthermore, once adopted, the current process for analyzing voluntary commitments, drawing comparisons amongst TLDs, measuring effectiveness, and building data points for analysis, is too cumbersome because such commitments are only available in individualized contractual documents embedded on the ICANN website and not available in a categorized, searchable form. Unlike many other aspects of registry agreements, voluntary PICs vary greatly from one TLD to another. Therefore, a publicly accessible, categorized, searchable database of these commitments would enhance data-driven policy development, Community transparency, compliance, awareness of variables relevant to DNS abuse trends, and the overall ability of future review teams to measure their effectiveness.

**To**  
ICANN organization,  
New gTLD Subsequent  
Procedures PDP  
Working Group

**Priority level**  
Prerequisite

**Success measures:** The implementation of this recommendation would be successful if the purpose of any voluntary commitment proposed by a registry operator is clearly stated to describe its intended goal, all parties in the multistakeholder community are given ample time to provide input before such a commitment is adopted into a contract, and any adopted measures are available and easily accessible on the ICANN website in an organized way to empower Community awareness and accountability.

2017 RySG comment: This is a worthy goal, but latitude must be maintained following the application process for potential registries to add to voluntary PICs. It's not reasonable to assume every situation addressable by a voluntary PIC can be foreseen, as registries can attest from the 2012 round. What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

RySG comment:

The RySG reiterates its comments from 2017. While we understand the review team's point about providing the ICANN community time to review such voluntary commitments, this recommendation would prevent future applicants from being able to adopt such commitments in response to feedback from the community or individual parties after applying for a gTLD but prior to delegating it. There may be value in providing such a capability.

## Chapter IX. Safeguards

### Recommendation 26:

A study to ascertain the impact of the New gTLD Program on the costs required to protect trademarks in the expanded DNS marketplace should be repeated at regular intervals to see the evolution of those costs over time. The CCT Review Team recommends that the next study be completed within 18 months after issuance of the CCT final report, and that subsequent studies be repeated every 18 to 24 months.

The CCT Review Team acknowledges that the Nielsen survey of INTA members in 2017 was intended to provide insight into this topic but yielded a lower response rate than anticipated. The Team recommends a more user-friendly and perhaps shorter survey to help ensure a higher and more statistically representative response rate.

#### Rationale/related findings:

Costs will likely vary considerably over time as new gTLDs are delegated and registration levels evolve. Repeating the Impact Study would enable a comparison over time.

**Details:** The evolution of costs required to protect trademarks over time will provide a more precise picture of the effectiveness of RPMs generally in the DNS.

**Success measures:** The results of future impact studies should provide significantly more data to the relevant working groups currently looking into RPMs and the TMCH, as well as to future working groups, thereby benefiting the Community as a whole. Recommendations would then also be able to evolve appropriately in future CCT Review Teams.

To  
ICANN organization

Priority level  
High

Jan 2018 RySG comment: The RySG recognizes the value in conducting this type of impact study, and that the complexity of the INTA Impact Study made it difficult for many respondents to complete the questionnaire.

Going forward, ICANN should take steps to ensure that any studies conducted are optimized to solicit meaningful and statistically significant data from a representative sample of respondents.

#### RySG comment:

The RySG reiterates its 2018 comments.

## Chapter IX. Safeguards

### Recommendation 27:

Since the Review Team's initial draft recommendation, the PDP Review of All RPMs in All gTLDs Working Group started reviewing the URS in detail and, at the time of writing, their review is ongoing. Given this ongoing review, the Review Team recommends that the Working Group continue its review of the URS and also looks into the interoperability of the URS with the UDRP.

The review team encountered a lack of data for complete analysis. The PDP Review of All RPMs appears to also be encountering this issue and this may well prevent it from drawing firm conclusions. If modifications are not easily identified, then the CCT Review Team recommends continued monitoring until more data is collected and made available for review at a later date.

**Rationale/related findings:** It is important for all gTLDs to have a level playing field, so the applicability of the URS should be considered for all gTLDs.

**Details:** A review of the URS should explore potential modifications, such as: (1) whether there should be a transfer option with the URS rather than only suspension; (2) whether two full systems should continue to operate (namely the UDRP and URS in parallel), considering their relative merits; (3) the potential applicability of the URS to all gTLDs; and (4) whether the availability of different mechanisms applicable in different gTLDs may be a source of confusion to consumers and rights holders.

**Success Measures:** Based on the findings, a clear overview of the suitability of the URS and whether it is functioning effectively in the way originally intended.

To  
GNSO

Priority level  
Prerequisite

2017 RySG comment: *What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?*

Jan 2018 RySG comment: It appears that this recommendation is already being followed through the work of the RPM PDP WG, which is reviewing the URS.

In support of ICANN's policy development process, and for the sake of avoiding duplication of efforts, the RySG believes that allowing the RPM PDP WG to proceed with its work is sufficient to meet this recommendation. However, the RySG notes that the CCT-RT has only provided a list of suggestions, but no information as to what issues or problems led to them. We believe it would be very helpful to the RPM PDP to include a reason for each suggestion.

We trust that the GNSO Council will duly consider the findings and recommendations that the RPM PDP WG produces in its Final Report regarding its phase one review of new gTLD RPMs.

RySG comment:

The RySG reiterates its 2018 comments.

**Chapter IX. Safeguards**

**Recommendation 28:**

**A cost-benefit analysis and review of the TMCH and its scope should be carried out to provide quantifiable information on the costs and benefits associated with the present state of the TMCH services, and thus to allow for an effective policy review. Since the review team’s initial draft recommendation, the PDP Review of All RPMs in All gTLDs Working Group has started reviewing the TMCH in detail and ICANN has appointed Analysis Group to develop and conduct the survey(s) to assess the use and effectiveness of the Sunrise and Trademark Claims RPMs. Provided that the PDP Working Group has sufficient data from this survey or other surveys and is able to draw firm conclusions, the review team does not consider that an additional review is necessary. However, the CCT Review Team reiterates its recommendation for a cost-benefit analysis to be carried out if such analysis can enable objective conclusions to be drawn. Such cost-benefit analysis should include, but not necessarily be limited to, looking at cost-benefits of the TMCH for brand owners, registries, and registrars now and going forward, as well as examine the interplay of the TMCH with premium pricing.**

**Rationale/related findings:** The Independent Review of Trademark Clearinghouse (TMCH) Services Revised Report was unable to provide definitive conclusions on the relative utility of the TMCH due to data limitations. Analysis Group noted in the report that it was unable to perform a cost-benefit analysis of extending the Claims Service or expanding the matching criteria.

**To**  
GNSO

**Priority level**  
Prerequisite

**Details:** There appears to be considerable discussion on whether the TMCH should be expanded beyond applying to only identical matches and if it should be extended to include or common typographical errors of the mark in question. If an extension is considered valuable, then the basis of such extension needs to be clear.

**Success Measures:** The availability of adequate data to make recommendations and allow an effective policy review of the TMCH.

2017 RySG comment:

We agree with a review of the TMCH—it was lauded as a system that would be put to extensive use by rights holders, but that is far from the actual case. What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

Jan 2018 RySG comment:

The RySG respectfully requests that the CCT-RT provide additional detail about how it believes such a cost-benefit analysis should be undertaken and what specific value it would add to the extensive evaluation of the TMCH already being undertaken by the RPM PDP WG. While the RPM PDP WG has been reviewing the TMCH, it has not engaged in any specific cost-benefit analysis. Given that the WG is still underway, in order for the GNSO to be able to adopt this recommendation, additional guidance from the CCT-RT would be helpful. The RySG also requests that the CCT-RT consider balancing the benefits of such an analysis with the time and resources required to undertake it.

RySG comment:

The RySG reiterates its comments from 2017 and 2018.



**Chapter X. Application and Evaluation Process of the New gTLD Program**

<p><b>Recommendation 29:</b>  <b>Set objectives for applications from the Global South</b></p>		
<p><b>Rationale/related findings:</b> Applications were few, but there was no concerted effort to encourage them.</p> <p><b>Details:</b> The New gTLD Subsequent Procedures Working Group needs to establish clear, measurable goals for the Global South, including whether or when applications and even number of delegated strings should be objectives. It is possible that short-term objectives should be around second-level participation.</p> <p><b>Success Measures:</b> Increased participation by the Global South as demonstrated by increased applications and delegations</p>	<p><b>To</b>  New gTLD Subsequent Procedures Working Group</p>	<p><b>Priority level</b>  Prerequisite - objectives must be set</p>
<p><u>2017 RySG comment:</u> What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?</p>		
<p><u>RySG comment:</u>  This recommendation attempts to remain neutral in its language around whether a higher number of applications and delegations from the Global South should be objectives of subsequent new gTLD procedures, but the Success Measures pre-suppose that an increase in applications and delegations is a desirable and agreed-upon. This is fairly presumptuous on the part of the review team.</p>		

**Chapter X. Application and Evaluation Process of the New gTLD Program**

<p><b>Recommendation 30:</b>  <b>Expand and improve outreach into the Global South</b></p>		
<p><b>Rationale/related findings:</b> Low understanding of New gTLD Program in the Global South</p> <p><b>Details:</b> If increased applications from the Global South is determined to be an objective for a future round of applications, outreach to the Global South requires a more comprehensive program of conference participation, thought leader engagement, and traditional media. The work of AMGlobal should be built upon to identify targets, outlets, and venues for better outreach. This outreach should include cost projections, potential business models, and resources for further information. Furthermore, the review team recommends that the outreach program begin significantly earlier to facilitate internal decision-making by potential applicants.</p> <p><b>Success Measures:</b> Ideally, success would be measured in appreciable growth in applications from the Global South. In the absence of such growth, ICANN should survey entities in the Global South again to determine the sources of the difficulties that continue to be faced by potential applicants.</p>	<p><b>To</b>                  ICANN organization</p>	<p><b>Priority level</b>                  Prerequisite</p>
<p><u>2017 RySG comment:</u> What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?</p>		
<p><u>RySG comment:</u>                  As with Recommendation 29, this recommendation pre-supposes that an increased number of applications and delegations from the Global South is a desirable and agreed-upon objective.</p>		

## Chapter X. Application and Evaluation Process of the New gTLD Program

<b>Recommendation 31:</b> <b>The ICANN organization to coordinate the <i>pro bono</i> assistance program.</b>		
<b>Rationale/related findings:</b> Despite the registration of both volunteers and applicants, there is no evidence of interaction.  <b>Details:</b> Again, if additional applications from the Global South is determined to be an objective of a future round, the <i>pro bono</i> assistance program would be coordinated by the ICANN organization to ensure that communication is successful between volunteers and applicants.  <b>Success Measures:</b> Both volunteers and applicants should be surveyed by the ICANN organization on the success of the interaction between them so that future reforms can be based on better information.	<b>To</b> ICANN organization	<b>Priority level</b> Prerequisite
<u>2017 RySG comment:</u> What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?		
<u>RySG comment:</u> The RySG reiterates its 2017 comment.		

**Chapter X. Application and Evaluation Process of the New gTLD Program**

<p><b>Recommendation 32:</b>  <b>Revisit the Applicant Financial Support Program.</b></p>		
<p><b>Rationale/related findings:</b> Only three applicants applied for support.</p> <p><b>Details:</b> The total cost of applying for a new gTLD string far exceeds the \$185K application fee. Beyond efforts to reduce the application fee for all applicants, efforts should be made to further reduce the overall cost of application, including additional subsidies and dedicated support for underserved communities.</p> <p><b>Success Measures:</b> Greater participation in the applicant support program.</p>	<p><b>To</b>  New gTLD Subsequent Procedures Working Group</p>	<p><b>Priority level</b>  Prerequisite</p>
<p><u>2017 RySG comment:</u> What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?</p>		
<p><u>RySG comment:</u>  The CCT Report clearly states that it was difficult to assess the effectiveness of the support program because there were only three applicants. The data the CCT-RT was able to obtain (through survey responses) cites the ongoing cost of operating a registry as a barrier to entry, rather than the application cost itself. As such, it is not clear how the CCT-RT reached the conclusion that the application fee should be reduced for all applicants.</p>		

**Chapter X. Application and Evaluation Process of the New gTLD Program**

**Recommendation 33:**

**As required by the October 2016 Bylaws, GAC consensus advice to the Board regarding gTLDs should also be clearly enunciated, actionable and accompanied by a rationale, permitting the Board to determine how to apply that advice. ICANN should provide a template to the GAC for advice related to specific TLDs, in order to provide a structure that includes all of these elements. In addition to providing a template, the Applicant Guidebook (AGB) should clarify the process and timelines by which GAC advice is expected for individual TLDs.**

**Rationale/related findings:** The early warnings provided by GAC members helped applicants to improve delegated gTLDs by ensuring that public policy or public interest concerns were addressed, and should continue to be an element of any future expansion of the gTLD space. Applicants could withdraw their applications if they determined that the response or action required to respond to GAC early warning advice was either too costly or too complex and to do so in a timely manner that would permit them to recover 80% of the application cost.

Where general GAC advice was provided by means of communiqués to the ICANN Board, it was sometimes not as easy to apply to the direct cases. Applying for a gTLD is a complex and time-consuming process and the initial AGB was amended even after the call for applications had closed. Given the recommendations to attempt to increase representation from applicants from the Global South, it would be appropriate to ensure that the clearest possible information and results from the last round were made available.

**Details:** While the details should be left to the Subsequent Procedures PDP Working Group, the CCT Review Team believes there should be a mechanism created to specifically allow objections and means to challenge assertions of fact by individual members of the GAC. Finally, some sort of appeals mechanism is imperative.

**Success measures:** This recommendation stems from a more qualitative assessment by the review team and anecdotal feedback from applicants. Consequently, the measures for success will be similarly qualitative as the next CCT Review Team evaluates the process of gTLD application moving forward. That said, the proof will lie in the implementation of the recommendation. With a structured process and template for the submission of GAC advice, and a process for objection and appeal, the most frequently voiced concerns of applicants regarding such advice will be addressed.

**To**  
Subsequent Procedures  
PDP Working Group,  
GAC, ICANN  
organization

**Priority level**  
Prerequisite

2017 RySG comment: What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

**RySG comment:**

RySG supports the recommendation in principle but has concerns about ICANN’s ability to implement it. Furthermore, the RySG strongly opposes the “detail” section which seems to go far beyond giving the GAC a template for consensus advice. The “Detail” section suddenly adds new features: a role for individual GAC countries to object and an appeals mechanism.

## Chapter X. Application and Evaluation Process of the New gTLD Program

<b>Recommendation 34:</b> <b>A thorough review of the procedures and objectives for community- based applications should be carried out and improvements made to address and correct the concerns raised before a new gTLD application process is launched. Revisions or adjustments should be clearly reflected in an updated version of the 2012 Applicant Guidebook.</b>		
<b>Rationale/related findings:</b> Given the assessment carried out by the Ombudsman's Own Motion Report, the results of community-based objections, the Council of Europe report on the human rights perspective of those applications, and the interest raised by the ICANN community regarding the relative lack of success of community-based applications (an area where the ICANN community had intended to provide a special entry for communities to gTLDs of particular interest and use for them), it could be expected that there would be a higher rate of success for community-based applications.	<b>To</b> Subsequent Procedures PDP Working Group	<b>Priority level</b> Prerequisite
<u>2017 RySG comment:</u> What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?		
<u>RySG comment:</u> The RySG believes that the New gTLD Subsequent Procedures PDP Working Group is already working on such a review of community-based gTLD applications. We support the PDP's ongoing work and caution that a Review Team should not attempt to pre-suppose the outcome of any policy development process.		

**Chapter X. Application and Evaluation Process of the New gTLD Program**

**Recommendation 35:**

The Subsequent Procedures PDP should consider adopting new policies to avoid the potential for inconsistent results in string confusion objections. In particular, the PDP should consider the following possibilities:

1. Determining through the initial string similarity review process that singular and plural versions of the same gTLD string should not be delegated.
2. Avoiding disparities in similar disputes by ensuring that all similar cases of plural versus singular strings are examined by the same expert panelist.
3. Introducing a post-dispute resolution panel review mechanism.

**Rationale/related findings:** From a review of the outcome of singular and plural cases, it would appear that discrepancies in outcomes arose because the dispute resolution process allowed for different expert panelists to examine individual cases, although they were based on similar situations. This meant that different expert panelists could come to different conclusions in cases that otherwise might have been considered to have similar characteristics

The ICANN Program Implementation Review found that there was no recourse after a decision was reached by an expert panel. Given that there appear to be inconsistencies in the outcomes of different dispute resolution panels, it would be useful to establish a review mechanism.

There appear to be inconsistencies in the outcomes of different dispute resolution panels regarding singular and plural versions of the same word, which should be avoided in order to avoid confusing consumers.<sup>620</sup>

**Details:** While the details should be left to the New gTLD Subsequent Procedures Working Group, the CCT Review Team believes there should be a mechanism created to specifically allow for objections by individual members of the GAC and means to challenge assertions of fact by GAC members. Finally, some sort of appeals mechanism is imperative.

**Success Measures:** No string confusion objections are filed for cases of singular and plural versions of the same string. Or, should singular and plural versions be allowed, objection panels evaluate all such cases with a consistent approach such that all single or plural disputes are resolved in the same manner.

**To**  
Subsequent Procedures  
PDP Working Group

**Priority level**  
Prerequisite

2017 RySG comment: What is the perceived benefit of this recommendation, what would the cost be to carry it out, and would the benefit exceed the cost?

RySG comment:

The RySG believes that the New gTLD Subsequent Procedures PDP Working Group is already working on such a review of community-based gTLD applications. We support the PDP’s ongoing work and caution that a Review Team should not attempt to pre-suppose the outcome of any policy development process.