# Competition, Consumer Trust and Consumer Choice Review (CCT)

**Final Recommendations briefing to SSR2**

**October 2018**

ICANN

# Summary

- 35 recommendations
- Full consensus reached on all recommendations
- 1 recommendation directed to SSR2, many others that are relevant

| Final Report Sections | # |
|---|---|
| Data-driven analysis: Recommendations for Additional Data Collection and Analysis | 1 |
| Competition | 6 |
| Consumer Choice | 3 |
| Consumer Trust | 3 |
| Safeguards | 15 |
| Application and Evaluation Process of the New gTLD Program | 7 |

# CCT Review Team

- Looked at consumer trust and safeguard issues which including topics that relate to the security and stability of the DNS
- Survey of Internet users established that users do care about trust and expect security when using the Internet, especially when conducting financial or health transactions
- Correlation between familiarity of a TLD and trust
- CCT analyzed the safeguards put in place as part of the new gTLD program and analyzed how consumer expectations met reality when it came to security issues in the form of DNS Security Abuse
- CCT also identified overlap between trademark infringement and DNS Security Abuse

# New gTLD Safeguards Related to Abuse

Prior to launching the program, the community identified the following areas of concern:

- How do we ensure that “bad actors” do not run registries?
- How do we ensure integrity and utility of registry information?
- How do we ensure more focused efforts on combating identified abuse?
- How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?

ICANN identified and recommended nine safeguards to mitigate these risks, of which CCTRT was tasked to assess the effectiveness:

1. Vet registry operators
2. Require Domain Name System Security Extension (DNSSEC) deployment
3. Prohibit “wildcarding”
4. Encourage removal of “orphaned glue” records
5. Require “Thick” WHOIS records
6. Centralize Zone File access
7. Document registry- and registrar-level abuse contacts and policies
8. Provide an expedited registry security request process
9. Create a draft framework for a high security zone verification program

# DNS Abuse

To measure the effectiveness of the technical safeguards developed for the New gTLD Program in mitigating various forms of DNS abuse, the CCT-RT commissioned:

**Statistical Analysis of DNS Abuse in gTLDs (SADAG) (9 August 2017)**

**Methodology**
Relied upon:

- Zone files,
- Whois records,
- 11 distinct domain name blacklist feeds

to calculate rates of technical DNS abuse from 1 January 2014 through the end of 31 December 2016.

The analysis includes:

1. Absolute counts of abusive domains per gTLD and registrar
2. Abuse rates
3. Abuse associated with privacy and proxy services
4. Geographic locations associated with abusive activities
5. Abuse levels distinguished by “maliciously registered” versus “compromised” domains
6. An inferential statistical analysis on the effects of security indicators and the structural properties of new gTLDs

# DNS Abuse

**CCT operating definition:** DNS abuse related to cybersecurity, such as malware distribution, phishing, pharming, botnet command-and- control, and high volume spam.

**Findings**

- Introduction of New gTLDs
  - → Did not increase the total amount of abuse for all gTLDs
  - → Decreased the number of spam associated registrations in legacy gTLDs
  - → Malicious registrations have increased (more common phenomenon in new gTLDs)

- Legacy vs. New gTLDs
  - → The nine new gTLD program safeguards alone did not prevent abuse
  - → Rates of abuse in legacy and new gTLDs were similar by the end of 2016
  - → Higher rates of compromised legacy gTLD domain names than new gTLDs
  - → Use of privacy/proxy services to mask registrant Whois data is more common in legacy than new gTLDs

- Abuse is neither universal nor random: abuse rates strongly correlated with registration restrictions imposed on registrants, and it appears registration prices may influence rates too

- When analyzing attributes of cross-TLD registry operators, the operators associated with the highest rates of abuse offered low price domain name registrations

- Domain names registered for malicious purposes often contained strings related **trademarked terms**

# Directed to SSR2

# Rec 16

**Recommendation**: 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.

# Rec 16

**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.

# Rec 16

**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.

**Prerequisite or Priority Level**: High

**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.

# DNS Abuse

# Rec 14

**Recommendation**: 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.[1]

**Rationale/related findings**: ICANN is committed to maintaining "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet."[2] 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.

# Rec 14

**Rationale/Related Findings (bis):** 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.

**To**: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, and the Subsequent Procedures PDP WG.
**Prerequisite or Priority Level**: High

**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.

# Rec 15

**Recommendation**: 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.

# Rec 15

**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. 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%), .gdn (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 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.

# Rec 15

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

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

**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 direct or 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.

# Rec 15

**Details (bis):** 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.

# Rec 15

**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.

# Rec 17

**Recommendation**: 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.

**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

**Prerequisite or Priority Level**: High

# Rec 17

**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.

# Rec 18

**Recommendation**[1]: 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?).

# Rec 18

**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.

**Prerequisite or Priority Level**: Medium

**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.

# Broader policy and information gathering

# Rec 7

**Recommendation**: 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.
**To:** ICANN organization

**Prerequisite or Priority Level:** High

**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.

# Rec 7

**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.

# Rec 10

**Recommendation**: 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.

**To:** Generic Names Supporting Organization

**Prerequisite or Priority Level:** Medium

**Consensus within team:** Yes

# Rec 10

**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.

# Rec 11

**Recommendation**: 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.

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

**Prerequisite or Priority Level:** Prerequisite

# Rec 12

**Rationale/related findings (ter):** 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.

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

**Prerequisite or Priority Level:** Prerequisite (incentives could be implemented as part of application process)

**Details:** In addition to benefits, 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 user's personal and sensitive information. They would also include an assessment of whether registration restrictions have had a negative impact on competition.

# Rec 13

**Recommendation**: 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:

1. Whether consumers and registrants are aware that certain new gTLDs have registration restrictions;

2. Compare consumer trust levels between new gTLDs with varying degrees of registration restrictions;

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;[1]

4. Assess the costs and benefits of registration restrictions to contracted parties and the public (to include impacts on competition and consumer choice); and

5. Determine whether and how such registration restrictions are enforced or challenged.

# Rec 13

**Rationale/related findings:** 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 Security Abuse levels correlate with strict registration policies, with bad actors preferring register domains with no registration restrictions. 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.

**To:** ICANN organization

**Prerequisite or Priority Level:** Low

# Rec 13

**Details:** 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. 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.

**Success Measures:** 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.

# Rec 19

**Recommendation**: 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.

**To:** Future CCT Review Teams

**Prerequisite or priority level**: Medium

**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.”

# Rec 20

**Recommendation**: 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.

# Rec 20

**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.

# Rec 20

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

**Prerequisite or Priority Level:** Medium

**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.

# Rec 21

**Recommendation**[1]: 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.[2]

**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.

# Rec 21

**Rationale/related findings (bis):**
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.

# Rec 21

**Rationale/related findings (ter):**
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.

**To:** ICANN organization

**Prerequisite or Priority Level:** High

**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.

# Rec 22

**Recommendation**: 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.

**To:** ICANN organization

**Prerequisite or priority level**: High

# Rec 22

**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.

# Rec 23

**Recommendation**: ICANN should gather data on new gTLDs operating in highly-regulated sectors to include the following elements:

- 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;
- 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;
- 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.
- 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.
- 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?).

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.

# Rec 23

**Rationale/related findings:** Although ICANN has implemented 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.

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

**Prerequisite or Priority Level:** High

# Rec 23

**Details:** 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. 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.

**Success Measures:** 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 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.

# Potentially relevant recommendations to SSR2

# Rec 24

**Recommendation**:
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.)

**To**: ICANN organization

# Rec 24

**Prerequisite or priority level:** Low

**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.

# Rec 25

**Recommendation**: 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.

# Rec 25

**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

**Prerequisite or priority level**: Prerequisite

# Rec 25

**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.

# Rec 26

**Recommendation**: 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.

**To:** ICANN organization

**Prerequisite or priority level**: High

# Rec 26

**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.

# Rec 27

**Recommendation**: 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.

**To:** Generic Names Supporting Organization

**Prerequisite or priority level**: Prerequisite

# Rec 27

**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 UDPR 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.

# Rec 28

**Recommendation**: 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:** Generic Names Supporting Organization

# Rec 28

**Prerequisite or 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 “mark+keyword” 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.

# Rec 33

**Recommendation**: 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.592 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 should clarify the process and timelines by which GAC advice is expected for individual TLDs.

**Rationale/related findings**: The GAC Early Warnings 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 percent of the application cost.[1]

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.[2] 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 are made available.[3]