The ICANN GNSO "Business Constituency"

Comment on Registration Directory Service (RDS-WHOIS2) Review Team Final Report

Status: FINAL
Version: 3.0
9-Dec-2019

Business Constituency Submission

GNSO//CSG//BC

Background

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter:

> The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:
>
> 1. promotes end-user confidence because it is a safe place to conduct business
> 2. is competitive in the supply of registry and registrar and related services
> 3. is technically stable, secure and reliable.

Business Constituency (BC) Comment on Registration Directory Service (RDS-WHOIS2) Review Team Final Report[1]

Thank you for the opportunity to comment in this important matter before the ICANN community. The BC wishes to thank the volunteer efforts of the members of the RDS-WHOIS2 Review Team (RT) for their assessment of the current gTLD Registry Directory Service (RDS) and whether its implementation has met the legitimate and necessary needs of law enforcement and promotes a technically stable, secure and reliable internet that promotes consumer trust while safeguarding registrant data.

Over the years, the BC has spearheaded or otherwise been involved with discussions regarding Whois and ICANN's responsibility to ensure the integrity and reliability of the RDS. More recently, the BC has collaborated with the community to assess the efficacy of RDS policy, and to share perspectives regarding harms arising from less-than-timely or -accurate access to accurate Whois information. The BC also has worked with other ICANN stakeholders to identify and develop policies for mitigating fraud and abuse harmful to end users -- whether business, non-commercial or individuals -- and sought to ensure the final RDS policy would reflect those concerns.

Prelude to the report: What ICANN Org and the community should do now to improve RDS

- With the number of registered domain names growing daily, it becomes vital to the security and stability of the DNS to ensure that registrant data is accurate. Accordingly, the BC urges the ICANN Compliance team to implement a proactive, methodical approach to winnowing inaccuracies. The team historically has been reactive and episodic in responding to Whois inaccuracy reports and in working with ICANN's GDD on the results of the Accuracy Reporting System (ARS). Compliance has the capabilities to research, analyze and enforce against inaccuracy in registration data when it sees suspected systemic issues, reported inaccuracy complaints, RDS accuracy studies, and DAAR reports and should be taking action without continual prompting.

[1] ICANN public comment page at https://www.icann.org/public-comments/rds-whois2-rt-final-report-2019-10-08-en/mail_form

- Further to the above, the community, regrettably, has witnessed failed or stalled accuracy initiatives. These community-driven initiatives, such as cross-field validation, must be implemented without delay.

- A record's inaccurate information can cause confusion and harm, especially if it is an act of identity theft. Inaccurate identity and contact information in the registration data go hand-in-hand with registrations that are perpetrating DNS abuse.

    - Eliminating the use of inaccurate data in any suspended domain name will add to the security and stability of the DNS. Inaccurate information would be excised from the registrant data.

    - In the light of the possibility that some contact fields may be eliminated or significantly reduced in scope, action should be undertaken to ensure that the registrant or the registrant's representative remain contactable and current.

- Synergies in the realm of Whois accuracy are available. The ARS sampled RDS records can be utilized for accuracy tests, while the Audit program samples registrars to conduct audits. No synergies appear to have been gained through separation of these action tracks.

- There are further opportunities to ensure Whois accuracy. The ARS appears to have been the only proactive measure to monitor existing Whois data quality. The data inaccuracy rate across the gTLD space, as confirmed by ARS, is still unacceptably high at 30-40%. The most common identifiable cause of inaccuracy is registrars' failure to validate and verify Whois data at the outset, which is easily remediable.

- Risk-based actions -- meaning that to the extent possible, risk assessment is performed *before* action is taken -- would be welcomed. This would ensure that all policies are assessed, audited, tracked, reported and enforced by the ICANN Compliance team.

Specific comment on Review Team recommendations

The BC offers comment on the following RT recommendations:

Recommendation R4.1

> The ICANN Board should initiate action to ensure ICANN Contractual Compliance is directed to proactively monitor and enforce registrar obligations with regard to RDS (WHOIS) data accuracy using data from incoming inaccuracy complaints and RDS accuracy studies or reviews to look for and address systemic issues. A risk-based approach should be executed to assess and understand inaccuracy issues and then take the appropriate actions to mitigate them.

BC Comment

ICANN Compliance indeed should adopt a more proactive stance in its review and assessment of inaccuracy complaints. When the RT interviewed the Compliance team, it was clear that the team -- while it reviewed every complaint and took action when appropriate -- did not look further to determine whether there existed similar inaccuracy issues, including general or systemic, with the associated registrar.

Though the language in this recommendation may be somewhat weak, its risk-based approach is intended to broaden the Compliance team's investigatory capability in the process of receiving and reviewing an inaccuracy complaint. For example, Compliance could investigate the following:

- Are there other domain names registered with the same underlying information?
- Is there a history with this registrar of a high number of inaccuracy complaints, as compared to the number of registrations it manages?
- Is the inaccurate information obviously incomplete or false?

Recommendation R4.2

The ICANN Board should initiate action to ensure that ICANN Contractual Compliance is directed to cross-reference existing data from incoming complaints and studies such as the ARS to detect patterns of failure to validate and verify RDS (WHOIS) data as required by the RAA. When such a pattern is detected, compliance action or an audit should be initiated to review compliance of the Registrar with RDS (WHOIS) contractual obligations and consensus policies.

BC Comment

Discussions with the Compliance team make clear that it did not review all sources of information to investigate and mitigate systemic inaccuracy abuse. Each case is evaluated individually and separately based upon the complaint itself. and proactive investigation is not performed.

Proactive investigation using all the data sources available to detect systemic abuse should be a routine function of the Compliance team.

Recommendations regarding Whois accuracy, as derived from the WHOIS1 Final Report

WHOIS1	Has Been	Rationale
Rec #5	Fully-implemented	However, effectiveness in improving RDS (WHOIS) accuracy still needs to be assessed.
Rec #6	Partially-implemented	Because the ARS project is still ongoing, and the identity accuracy checks originally proposed as Phase 3 have not yet been implemented.
Rec #7	Partially-implemented	Because "Substantial Failure" and "Full Failure" rates are missing from Annual reports on WHOIS improvements.
Rec #8	Partially-implemented	Because enforcement only happens when there is an RDS (WHOIS) inaccuracy complaint or an ARS-generated inaccuracy report, the review team does not believe this is a proactive approach to enforcing contractual obligations related to RDS (WHOIS) accuracy.
Rec #9	Not implemented	Because there has been no metrics-based assessment of overall RDS (WHOIS) data quality improvement, through either WDRP or other alternative policies to achieve Recommendation #9's objective of improving data quality.

BC Comment

The RT found that Recs. 6-8 are only partially implemented, and Rec. 9 was not implemented at all. The WHOIS1 RT final report was delivered in May 2012 and ICANN -- for 7½ years -- has not made sufficient changes to fully implement four of these five recommendations. With implementation of the Temp Spec and the present lack of visibility of registrant data, the accuracy issue is most likely worse than when the RT did its review.

The Compliance team, outside of the ARS, does not collect sufficient metrics to perform a proactive assessment that would result in improvement in data quality. This is an overarching problem with implementation of ICANN policies.

Recommendation R5.1

The Accuracy Reporting System, which was instituted to address concerns regarding RDS (WHOIS) contact data accuracy, has demonstrated that there is still an accuracy concern and therefore such monitoring must continue. ICANN organization should continue to monitor accuracy and/or contactability through either the ARS or a comparable tool/methodology.

BC Comment

Although GDPR and the Temp Spec have impacted the ability to review accuracy and quality of registrant data, it remains a core ICANN responsibility to ensure the stability and security of the internet. ICANN must have access to the registrant data and play a central role in its availability, accuracy and integrity.

Recommendation R10.1

The Board should monitor the implementation of the PPSAI. If the PPSAI policy does not become operational by 31 December 2019, the ICANN Board should ensure an amendment to the 2013 RAA (or successor documents) is proposed that ensures that the underlying registration data of domain name registrations using Privacy/Proxy providers affiliated with registrars shall be verified and validated in application of the verification and validation requirements under the RAA unless such verification or validation has already occurred at the registrar level for such domain name registrations.

BC Comment

At the time of the review, the PPSAI IRT was working toward policy implementation. Notwithstanding ICANN unilaterally pausing the IRT, this recommendation remains critical.

When GDPR was implemented in 2018 it was believed that many registrants would no longer utilize proxy and privacy services. Now, eighteen months later, the available data establishes a dramatic *increase* in privacy/proxy registrations to more than 40% of all registrations. In fact, certain registrars have implemented privacy/proxy registrations for all registrations instead of redacting the registrant data to comply with the Temp Spec.

Since the PPSAI policy has not been implemented, there is little recourse to gain access to this essential information beyond a formal legal proceeding.

At the very least there are important pieces of the PPSAI that should be implemented immediately. The PPSAI final report recommends indicating a privacy/proxy registration in the RDS. Because of current registrar practices, there is difficulty in determining whether registrant data is redacted or is a privacy/proxy registration.

If a third party requests the registrant data for what it believes is a redacted registration record, a registrar can claim that it is a privacy/proxy registration without any recourse for transparency.

Recommendation SG.1

The ICANN Board should require that the ICANN org, in consultation with data security and privacy expert(s), ensure that all contracts with contracted parties (to include Privacy/Proxy services when such contracts exist) include uniform and strong requirements for the protection of registrant data and for ICANN to be notified in the event of any data breach. The data security expert(s) should also consider and advise on what level or magnitude of breach warrants such notification.

In carrying out this review, the data security and privacy expert(s) should consider to what extent GDPR regulations, which many but not all ICANN contracted parties are subject to, could or should be used as a basis for ICANN requirements. The ICANN Board should initiate action intended to effect such changes.

The ICANN Board should consider whether and to what extent notifications of breaches that it receives should be publicly disclosed.

BC Comment

With data breaches reported daily by internet websites, the RT asked how many data breaches of registrars had occurred. ICANN does not currently collect this information, and there is no current requirement for a registrar to report data breaches to ICANN. This reporting is critical for the protection of registrant data, and the BC recommends such a requirement.

Recommendation CC.1

The ICANN Board should initiate action intended to ensure that gTLD domain names suspended due to RDS (WHOIS) contact data which the registrar knows to be incorrect, and that remains incorrect until the registration is due for deletion, should be treated as follows:

(1) The RDS (WHOIS) record should include a notation that the domain name is suspended due to incorrect data; and

(2) Domain names with this notation should not be unsuspended without correcting the data.

BC Comment

This recommendation would prevent a domain name suspended for inaccurate data from being reinstated without updating the record with accurate data. The requirement of indicating in the RDS that the domain was suspended due to inaccuracy will be helpful in collecting metrics on inaccuracy.

Recommendation CC.2

The ICANN Board should initiate action intended to ensure that all gTLD domain name registration directory entries contain at least one full set of either registrant or admin contact details comparable to those required for new registrations under the 2013 RAA (or any subsequent version thereof) or applicable policies.

BC Comment

Domain names registered before the 2013 RAA must comply only with the 2009 RAA, which did not require the Registrant contact information to provide an email address or phone number. According to the ARS report, 30% of all gTLD domain names are "grandfathered" registrations, subject only to 2009 RAA requirements. According to EPDP discussions, registrant data may be the only information that will be required to collect in the near future. This could result in no email address or phone number in the registrant data record for 30% of the legacy TLDs, an unacceptable outcome.

Recommendation CC.3

The ICANN Board should take steps to ensure that ICANN Contractual Compliance is adequately resourced factoring in any increase in workload due to additional work required due to compliance with GDPR or other legislation/regulation.

BC Comment

With the recent changes and staff departures on the Compliance team, this recommendation is more critical.

Recommendation CC.4

The ICANN Board should recommend the GNSO adopt a risk-based approach to incorporating requirements for measurement, auditing, tracking, reporting and enforcement in all new RDS policies.

BC Comment

The RT was surprised that regarding several of the policies that had been implemented since the last WHOIS RT report there were no statistics or metrics collected by ICANN. It is therefore difficult to assess the impact of and compliance with each policy. This recommendation would require every new policy to include rationale and best practices for measurement of the critical statistics of the policy once implemented, an outcome the BC supports.

Steps forward

- The BC believes the ICANN Board should move quickly to adopt all of the RDS Review Team's Recommendations.

- ICANN hasn't made sufficient changes to fully implement the first Review Team's recommendations in the last 7½ years. The BC calls for immediate implementation of the first RT's recommendations.

- The BC singles out Recommendation 10 of the report (privacy/proxy services) and signals its strong, unqualified agreement. It is preposterous to further delay implementation of community recommendations while cybercriminals benefit from ICANN's stalling.

- The Temp Spec and lack of transparency of registrant data most likely has made the accuracy issue worse than when the Review Team did its review. The BC believes ICANN Org must redouble its efforts to ensure accuracy and integrity of data records.

- ICANN must fully implement community recommendations, update contracts where necessary, adequately staff its Compliance function (particularly after recent staffing changes) and establish measurable metrics for RDS policy.

- As noted above, the Compliance team's work is too siloed, episodic and reactive. Compliance should proactively review and cross-reference all sources of information to investigate and mitigate systemic inaccuracy abuse.

- Though GDPR and the Temp Spec impacted this capability, one of ICANN's core responsibilities is to ensure and protect accuracy and data quality and integrity in registrant data. ICANN must have access to the registrant data and play a central role in the availability of the data.

- ICANN must resume publication of the Accuracy Reporting System's periodic reports on WHOIS accuracy.

- We agree that a domain name suspended for inaccurate data must not be reinstated without updating the record with accurate data. Indicating in the RDS that the domain was suspended due to inaccuracy will be helpful in collecting metrics on inaccuracy.

--

This comment was drafted by Mason Cole, Margie Milam, Susan Kawaguchi, and Ben Milam.

It was approved in accord with the BC Charter.