SSR2 Review Questions, Batch 2
By GDD February 2019

Question 6: The SSR1 review team called out a number of activities that were operational and within staff's purview and contained in the SSR framework and called for implementation of measurements and metrics. Was that work done and is it captured anywhere? To clarify, as part of the SSR1 report related to rec 11, the SSR1 review team noted ICANN administration of the new gTLD Program, IDN program, significant SSR related issues that are in the framework. They called for more specific goals, measurements and impact assessment. Was that work done and is it captured somewhere else?

Answer:

There are two distinct levels which could be reviewed. The top-level and the second level.

For the top-level, the existing processes for gTLD and IDN ccTLD reviews already contain DNS Stability review and string similarity review (the latter process is comprised on multiple panels for IDN ccTLDs). In addition, ICANN org has been working with the community to conduct a much more detailed analysis under the RZ-LGR project. RZ-LGR has a significant focus on security and stability aspects of TLD labels.

ICANN has also been supporting work for the second level. It has worked with the community to update the IDN Guidelines to version 4.0, based on the knowledge which the community has gathered on IDNs since 2011 when version 3.0 for these guidelines were approved. IDN Guidelines 4.0 adds many more requirements for the registries which are relevant for SSR2 (see detailed Guidelines for a comprehensive overview), which address the consumer confusion aspects of second level IDN labels. In addition, ICANN is also developing reference IDN Tables for the second level which are pre-vetted for security and stability for the registries to consider adopting.

For the second level, with regards to the operations, ICANN checks IDN tables for all registries which intend to offer second level domains from security and stability perspective, thus limiting the IDN labels which can be generated.

Several processes that were developed as part of the New gTLD program were related to SSR. These were listed in the prior report. These processes are still supported and expect to be in use until the end of the 2012 round. Additional processes such as the Emergency Back End Registry Operator (EBERO) and Trademark Clearinghouse (TMCH) continue to be supported and have been updated over time as new requirements and process improvement are identified. Below are updates to the metrics given in the prior report. (Highlighted stats are new).

Evidence / Measures the requirements were effective	
Total Applications Received	1930
Applications placed into contention by String Similarity Panel / Contention Sets Created	754 Applications / 234 Contention Sets
Strings not approved for delegation due to risk of name collisions	3
String Confusion Objections filed/ Objector Prevailed (contention created or application eliminated)	67 / 12
Legal Rights Objections Filed / Objector Prevailed (application eliminated)	69 / 5
Potential Number of Unique Strings to be delegated (30 June 2018)	1246

Registry Agreements executed ((30 June 2018)	1232 (99% of potential)
gTLD's successfully completed PDT (30 June 2018)	1232 (99% of potential)
gTLD's Delegated to Rootzone (30 June 2018)	1231 (99% of potential)

Note there has been one EBERO event since the start of the New gTLD program.

There has also been Pre-Delegation Testing which also has some additional checks for SSR.

Pre-Delegation Testing (PDT) was designed to ensure that a new Registry Operator had the technical capability to operate a registry. It included testing of the 5 critical registry functions. Testing itself was a mix of self-certification, manual testing and automated testing. Registries that had issues with testing were required to correct the issue before they could complete testing. All Registries that were delegated into the root zone passed PDT. Registries that change their back-end operator may also require testing depending on the qualifications of the provider. The requirements to pass PDT have been updated several times over the years as new policy requirements come into effect. The most recent changes were due to the Temporary Specification and the acceptance of LGR formatted IDN tables.

Question 7: What measurements exist, and are used, for the effectiveness of mechanisms to mitigate domain name abuse, as required in recommendation 11?

Answer:

Recommendation 11: ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse.

Please refer to reports on this page: https://newgtlds.icann.org/en/reviews/cct/dns-abuse when it comes to the New gTLD Program. The potential measurements and data available vary across the mechanisms discussed; However, several statistics have been gathered and are included in these reports.

For the Domain Abuse Activity Reporting project, please refer to this page: https://www.icann.org/octo-ssr/daar.

Question 9: Please provide information on data escrow providers" contractual obligations/requirements and actions taken by ICANN Org. to monitor and ensure compliance with these obligations

Answer:

Registry Operators operating under the 2017 base New gTLD Registry Agreement and similar forms are required to have a Data Escrow Agreement with an ICANN approved Data Escrow Agent. The agreement must name ICANN as a third-party beneficiary as per Specification 2 of the Registry Agreement. The contractual obligation of Registry Data Escrow Agents are outlined in the Registry Escrow Agreements, which are reviewed, approved by ICANN and posted here. As per the Registry Escrow Agreement, Registry Data Escrow Agents are obligated to provide various data escrow deposit notifications to ICANN which are monitored by ICANN's Contractual Compliance department.

Registrars accredited under the 2013 Registrar Accreditation Agreement are required to make data escrow deposits according to Section 3.6. The contractual obligations of Registrar Data Escrow Agents (DEAs) are outlined in the Registrar Data Escrow Agreement (RDEA), which incorporates the RDE Specifications by reference. The approved RDEA templates of all Registrar DEAs are linked in on the Registrar Data Escrow Program page on icann.org. Pursuant to the RDEA, Registrar DEAs are required to send deposit reports to ICANN which are monitored by ICANN's Contractual Compliance department.

Question 10: Although this particular abuse report did not make any conclusions regarding the effectiveness of safeguards that were introduced by the New gTLD Program, one would come to the conclusion after reading this report that if the new gTLD safeguards have been effective, there would have been an observable reduction in the level of malicious registrations in new gTLDs compared to the legacy TLDs. That of course wasn't the case. Is staff drawing any conclusions, or has the result of this study generated any new areas that staff is exploring in terms of abuse and new gTLD safeguards?

Answer:

The Competition, Consumer Trust, and Consumer Choice Review Team (CCTRT) requested the SADAG study, and limited its scope to examining rates of domain names used for malware, phishing, and spam in new and legacy gTLDs.[1] However, in its deliberations, the Review Team utilized the phrase "DNS Abuse" more generally as an encompassing term to refer to "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names."[2] The CCTRT explicitly distinguished this general terminology from "DNS Security Abuse," which refers to specific, technical forms of abusive behavior such as malware distribution, phishing, pharming, botnet command-and-control, and spam. As the CCTRT noted:

Bad actors have misused…universal identifiers for cybercrime infrastructure and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud. Each of these activities may constitute a form of DNS abuse. Determinations as to how to characterize these forms of abuse depend largely upon local laws, the roles played by other infrastructure providers, and subjective interpretations. Nonetheless, consensus exists on what constitutes DNS Security Abuse, or DNS Security Abuse of DNS infrastructure, as demonstrated by

[1] SIDN Labs and the Delft University of Technology (August 2017), *Statistical Analysis of DNS Abuse in gTLDs Final Report*, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf
[2] CCTRT Final Report, p. 8 (footnote 11)

community findings associated with the development of the New gTLD Program. These forms of abuse include more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse.[3]

When discussing the scope of the then forthcoming SADAG study, the CCTRT acknowledged the wide range of activities that may constitute "DNS Abuse" based on the general definition above, but was constrained by the practical matter of gathering and analyzing data on quantitatively measurable forms of abuse.[4] A number of organizations monitor spam, phishing, and malware domains, and provide the results of that monitoring via domain blacklists. Through comparison of data provided by these organizations with zone file and WHOIS data, the SADAG researchers were able to produce the quantitative results seen in their study.

However, the nine New gTLD Program safeguards examined in the "DNS Abuse" section of the CCTRT Final Report were not specifically intended to mitigate spam, phishing, malware, or other forms of "DNS Security Abuse" as defined by the CCTRT.[5] These safeguards are:

1. Vetting of registry operators
2. Requirement for Domain Name System Security Extension (DNSSEC) deployment
3. Prohibition of "wildcarding"
4. Removal of "orphan glue" records
5. Requirement for "Thick" WHOIS records
6. Centralized Zone File access
7. Documented registry- and registrar-level abuse contacts and policies
8. Provision of an expedited registry security request process
9. Creation of a draft framework for a high security zone verification program

[3] Ibid., p. 88.
[4] As noted on p. 92 of the Report: "[A] challenge is the lack of data available regarding certain types of abuse. Nonetheless, there are core abusive behaviors for which there is both consensus and significant data available. These include spam, phishing, and malware distribution."
[5] These safeguards were originally proposed in the *Exploratory Memorandum: Mitigating Malicious Conduct*, (3 October 2009), https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

Regarding these safeguards, the CCTRT concluded:

> The results [of the SADAG study] demonstrate that the nine aforementioned safeguards alone do not guarantee a lower rate of abuse in each new gTLD compared to legacy gTLDs. Instead, factors such as registration restrictions, price, and registrar-specific practices seem more likely to affect abuse rates.[6]

The CCTRT also examined parts 3(a) and 3(b) of Specification 11, "Public Interest Commitments," in the New gTLD Registry Agreement. These provisions include language that addresses some of the technical forms of abuse that constitute "DNS Security Abuse" as defined by the CCTRT, copied here:[7]

> a. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.
>
> b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

---

[6] CCTRT Final Report, p. 94.
[7] See "Registry Agreement: Public Interest Commitments: Specification 11, parts 3(a) and 3(b)," https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#specification11

In regard to part 3(a), the CCTRT noted:

> ... the plain language of the safeguard does not obligate the registry operator to monitor and enforce this provision beyond requiring the inclusion of the provision in the downstream Registrar–Registrant agreement. ICANN has concluded that 99 percent of new gTLD registry operators had complied with the obligation to include this language in their Registry-Registrar agreements by the end of 2014.[8]

In regard to part 3(b), the CCTRT noted:

> The obligation to engage in security checks can be enforced, as implemented. ICANN Contractual Compliance reports engaging in proactive monitoring of this safeguard and determined, for example, that 96 percent of registries were conducting security checks as per the contract. Additionally, a voluntary "Framework for Registry Operator to Respond to Security Threats" has been released during the writing of this report.[9]

As a complement to Specification 11 and parts 3(a) and (b) of the Registry Agreement, the 2013 Registrar Accreditation Agreement bound new gTLD registrars to promptly "investigate and respond appropriately to any reports of abuse."[10]

The CCTRT reviewed ICANN's Contractual Compliance Annual Reports, which stated that registrar-level complaints involved "registrars not taking reasonable and prompt steps

[8] CCTRT Final Report, p. 106.
[9] Ibid., p. 107. See also: "Framework for Registry Operator to Respond to Security Threats," https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en)
[10] Ibid., p. 106. See also: "Registrar Accreditation Agreement, Section 3.18: Registrar's Abuse Contact and Duty to Investigate Reports of Abuse," https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa

to respond to appropriately to reports of abuse, which at a minimum should be to forward valid complaints to the registrants."[11] The CCTRT noted:

> ICANN's 2015 audit of registrars under the 2013 RAA indicated that 74 percent of the registrars audited had deficiencies related to the RAA contract provisions requiring a Registrar Abuse Contact and a duty to investigate complaints of abuse. ICANN's 2016 audit of registrars showed a deficiency rate of 60 percent related to this same contract provision. These figures indicate that the "mitigating abuse" safeguard is the subject of complaints and the ICANN compliance process.
>
> It is not clear whether these safeguards have had an impact on mitigating abuse. It is also not clear what constitutes "reasonable and prompt steps to respond to appropriately to reports of abuse.[12]

In regard to the above safeguards, the CCTRT concluded that, "Ultimately, the safeguards put in place as part of the [New gTLD] Program were too narrow in scope to prevent some of the malicious abuse issues identified prior to the introduction of the new gTLDs."[13]

As a result of this conclusion, the CCTRT proposed:

> ... the development of mandates as well as incentives to reward best practices that curb or prevent technical DNS Security Abuse and strengthen the consequences for culpable or complacent conduits of technical DNS Security Abuse. These recommendations may be applicable to curb other misuse of domain names to the extent the community reaches consensus on other forms of DNS abuse.[14]

---

[11] Ibid., p. 107. See also: "Contractual Compliance Annual Reports," https://www.icann.org/resources/pages/compliance-reports-2018
[12] Ibid., p. 106.
[13] Ibid., p. 9.
[14] Ibid., p. 97.

The details of these recommendations are contained primarily in recommendations 14 through 20 of the CCTRT's Final Report.[15]

Insofar as ICANN org's exploration of DNS abuse and its relationship to New gTLD Program safeguards is concerned, the org will continue to support community discussions of modified or new safeguards as a result of these and any other community-driven recommendations.

ICANN's Office of the CTO (OCTO) has built the "Domain Abuse Activity Reporting" (DAAR) system, which employs a methodology similar to that used in the SADAG study on an ongoing basis.[16]

After many informal requests from the community, OCTO concluded that the ICANN community would benefit from having a neutral, unbiased, persistent, and reproducible set of data from which analyses could be performed. OCTO began a research project to develop a system to collect a very large body of registration data, complemented by a large set of high-confidence reputation data feeds, so that the data collected by this system could serve as a platform for studying daily or historical registration or abuse activities and for reporting activity.[17]

[15] See pp. 17-20.
[16] See icann.org, "Domain Abuse Activity Reporting," https://www.icann.org/octo-ssr/daar
[17] See icann.org, "Frequently Asked Questions: ICANN's Domain Abuse Activity Reporting (DAAR) Project," https://www.icann.org/octo-ssr/daar-faqs/#why