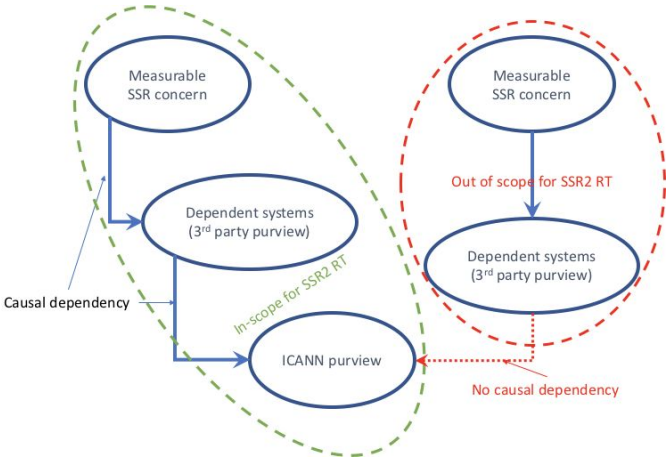
SSR2 RT – DNS SSR Work Stream

This work stream relates to Bylaw 4.6(c) (ii) A, 4.6(c) (ii) B, 4.6(c) (ii) C, and 4.6(c) (iii) and focused on the effectiveness of ICANN's stewardship over the areas of the Internet's globally unique identifier systems over which ICANN has purview. The evaluation of this effectiveness necessarily considers performance indicators, measures, and metrics that span administrative domains and operations that include (but are not limited to) ICANN. However, the focus of this work relates only to those systems within ICANN's remit.

Methodology Statement

The methodology of this sub-team focuses on the identifier systems which the review will evaluate: the global DNS, the IANA numbers databases (IP allocations and ASNs), and the IANA protocol registries. As each of these areas support complex networked systems to different degrees and in very different ways, the evaluation of them must be done in varying ways. Understanding the *way* that these identifiers are used is a critical component in evaluating "the effectiveness of the security efforts to deal with actual and potential challenges..." In part, this becomes necessarily complicated to measure because, for example, abuse in a user-facing application could conceivably only be possible because of an otherwise seemingly innocuous feature of a supporting component of the globally unique identifier system.

In order to evaluate the complex and multidimensional nature of the globally unique identifier system, its usage is a critical consideration. Therefore, the methodology to evaluate its SSR (for those portions under ICANN's purview) must start by broadly considering actual concerns, threats, attacks, abuse, other dependent signals and then mapping those signals to the relevant ICANN component(s), procedures, policies, etc. Due to the nature and complexity of abuse and SSR signals, it is anticipated that there might be multiple systems, policies, or other enabling components that work together. Those elements or systems that enable or facilitate actions, behaviors, etc. are broadly considered to be "dependent systems." The extent to which there is a relation to elements that fall under ICANN's purview, and that relation is contributory to the signal, is the extent to which the signal is included in this evaluation. This logic is illustrated in the figure below. For example, abuse that includes a DNS component, but only at hierarchical level below ICANN's operations would not be a relevant consideration for this work stream. However, if that example abuse were only able to be effectuated because of contents of the DNS Root Zone, or because a registry was operating outside of contractual operational norms, then there would be a causal relationship whose relevance would fall within the remit of this review team's evaluation.



Issues

These qualitative concerns will be decomposed into more precise concerns, and those elements that fall within the purview of this work-stream (per the above) will result in recommendations.

Who needs to be interviewed, what questions do we need answered

Root Zone Mgmt

- kc: Data sharing / data release
  What data sharing and release is currently available.
  - http://www.root-servers.org (bottom has links to each root's stats page)
  - http://stats.dns.icann.org/hedgehog/ (B,L)
  - https://www.icann.org/search/#!/?searchText=root%20server%20statistics
  - http://www.dns.icann.org/imrs/stats/
  - Modulo that: query statistics, DDoS measurement stats
    Propose a set of specific stats that should be archived at specific periodicity and served from an ICANN managed repo.
    - Get an update from ODI, ITHI, etc.
- RH: DNS Root Crypto
  - For all of the below (and disruptive changes, in general): determine what the metrics for success are, and the go/no-go checklist criteria are. ***To be updated by kc***
  - Elliptic curve crypto
    Review DPS, and academic work on the efficacy of EC for DNSSEC
    Propose the identification of a process and timeline to achieve an algo roll to elliptic curve
  - DNSSEC below root. TLD DNSSEC deployment
    Outline the existing data sources for this (SecSpider et. al)
    Instantiate a repo/perma-link to stats for this
  - KSK roll frequency and process. Look at HSM replacement
    Lit search of past deliberations over whether to roll the KSK or not: KSK specified in SP 800-81-2 S11.2.4
    DPS to be amended with lessons learned (TO BECOME A CHECKLIST) from KSK rollovers and include process considerations of HSM replacement. Provide periodic audit reports of adherence to the DPS during KSK rollovers.
  - Periodic tabletop for rolling KSK
    ICANN to conduct and report results from periodic tabletop exercises of KSK rolls
- BK+ZK: BC - DR plan
  Ask for any references that point to this.
  Modulo the above, recommend that one be created, published, maintained, and followed (measured by audits)
- DM: Name collision
  Review autodiscover domain issue. Identify what the status quo is. Review lit on name collisions and status of NCAP

- LW+BK: Root zone change management (Verification, etc.)
  Review a document that outlines procedures being used.
  Assess whether this is well covered by existing reporting (ack if it is)
    - Sanity checks of requests
    - verification and authorization
- BK+LW: TLD label management
- BK+LW: NS / DS record management

Root server system (e.g. l-root)

- ~~l-root operations SSR~~
  ~~Review existing reporting (ODI, etc.) on l-root stats~~
  ~~https://www.dns.icann.org/imrs/~~
- AA: Best practice + System hardening of l-root
  Look for publications that indicate l-root's adherence to published best practices for RSOs. l-root management strategy
    - Published statement from l-root ops of harding that is done to infrastructure
    - l-root technical leadership (lead by example)
    - How is it being maintained, how is it being distributed, how do you obtain copies, site selection criteria, how do ops respond to incidents, what is the computation around increasing capacity
- ~~capacity to handle all root traffic~~
  ~~Look for published aggregate stats of global root traffic and global capacity of l-root~~
  ~~Ensure that stated capacity of l-root meets/exceeds global volume(s)~~
- Root server system protection: assess the threatscape of top threats (e.g. DDoS to the root system)
  Was the threatscape documented and shared with the community/RSOs?
    - https://www.icann.org/en/system/files/files/rssac-review-final-02jul18-en.pdf
- ~~Root server system evolution~~
  ~~Review existing root server ecosystem documentation to evaluate the need for further investigation~~
- kc: Comment on RSSAC document around proposed governance model for the root servers environment
  https://www.icann.org/en/system/files/files/rssac-037-15jun18-en.pdf (recommends a "Strategy, Architecture, and Policy Function" to offer guidance on matters concerning the RSS
    - "performance monitoring and measurement function" as part of new governance model.
    - https://www.icann.org/en/system/files/files/rssac-038-15jun18-en.pdf (asks ICANN to drive progress on implementation of above doc)
    - management process (gov)(RSSAC 0037 implementation)

Alternate Root Deployment and Co-Existence (DNSSEC makes alt. harder)

- EO: Accountability & Transparency with respect to risks and benefits - annual report
  Commision yearly studies that result in public reports of the state of alternate roots on the the Internet (risks/benefits)

- tracking and measurement (deltas etc.)
- Cannot police but can report public
- Impact vs. coexistence

SSR Measurements

Top-Level Domain SSR Measurement Reports
<>
IANA Registry SSR Measurement Reports
<>
Root Zone SSR Measurement Reports
<>

- KB: SLA compliance (SLAs for what?, with whom?)
  A mechanism to be put in place that measure SLA compliance: IANA services, TLD registries (covered in ICANN SSR), registrars (covered in ICANN SSR)
  A mechanism to track and verify that SLAs are being met.
- EO+kc: Propagation delay and consistency of changes of zone contents across name servers
- SM: IANA registry availability measurements - security
  Request a public documentation of the infrastructure and service-level SSR aspects of how IANA registries are served and maintained
  - Time zones?
- Identify KPI for SSR measurements
  Request / commision analysis of KPIs for the root (others)?

Namespace Abuse

- DM+kc+JM+NR: transparency with respect to abuse (is this DAAR?)
  Review the agreement and text of the CCT report (e.g. TLD abuse indicators)
  REcommend the further development of DAAR and how the *community* can measure it
  An actionable mechanism
  Mechanisms to evaluate the utility of this to the community
  - Abuse data made public with API for major threat vectors registries, registrars, each month
  - Public but delayed?
- DM: reactive vs. proactive compliance - one-off complaints response vs. data driven priorities
  DM to pull together relevant publications on this: CCT Review, RDS review, SAC0101, etc.
  - Best practices and potential requirements (eg. 2-factor for DNS)
    SAC074
    Should there be a security requirements for registrar accounts
    Raise awareness of best practices
    https://www.icann.org/en/system/files/files/sac-074-en.pdf

Point to implementation guidance (re SAC074) for user/registrar account access, etc…

- LW+NR+DM+kc: leadership
  Give ICANN compliance a “big stick” to lead abuse remediation initiatives and take action
  - Check the bylaws (and possibly suggest directions to change towards)
  - Take other review teams’ recommendations into consideration (RDS RT, CCT RT)
- NR+LW+EO: Proactive anti-abuse by registrars and registries
  Enshrine that the problem and the data are still around (though public whois is not), and this may have shifted the onus for solving/addressing this problem
- RH: IDN domain names (glyph phish)
  Information gathering on homoglyph attacks and threatscape
  Possibly: REcommend implementation of SAC0xx
  - Universal Acceptance (e.g. homoglyph attacks - browser / display, U+ ü, Canonical form (lack of), …)
  - Track the support in sw
- ~~IP space hijacking~~
  ~~Acknowledge as identifier abuse… An SSR concern…Propose partnership and research/investigation into remediations and longer term…~~

...

Software interop

- DNS over TLS (move to Futures)
- EO+LW: Testbed of software variants (NS / resolver / etc.) for regression testing
  Recommend that this facility be created, maintained, and used
- <meta comment for recommendations in this work stream>Before any delta define: metrics, checklist - make sure all boxes are checked
  - where are the procedures / tests? (applies to all)
    </meta comment for recommendations in this work stream>

Recommendations

<>