Remaining metrics for discussion

Metric	Description	Data source/considerations	Category
1.1	% DNS Service Availability (present SLA is 100%).	Data is reported to ICANN but must remain confidential.	
1.2	% Availability for Registration Data Directory Services (RDDS). (SLA is 98%)		
1.3	% of Service Availability for Shared Registration Services (SRS, using EPP). (SLA is 98%). Open TLDs only.		
1.5	% Uptime for Registrar services such as WHOIS, contact info, and complaints, assuming that SLAs are established for these measures in the new RAA.		Trust
1.11	Quantity of intellectual property claims and cost of domain name policing relating to new gTLDs. Relative incidence of IP claims made in good faith should be measured in 3 areas: IP claims against registrants regarding second level domains in new gLTDs; IP claims against registrars regarding Second level domains in new gTLDs; IP claims against new gTLD registries regarding second level domains and TLDs. Quantity of second level domains acquired because of infringement or other violations of IP rights of acquiring parties; and Cost of domain name policing and enforcement efforts by IP owners.	External, IAG-CCT members exploring feasibility with International Trademark Association (INTA,) which has expressed an interesting in polling their members on this topic. Subject to some definition of terms, such as which costs would be included, whether these are internal or external (in-house vs. outside counsel.)	Trust
1.14	Quantity and relative incidence of domain takedowns.	External, will require reporting from registries	Trust
1.15	Quantity and relative incidence of spam from domains in new gTLDs, which could be measured via specialized email addresses and methodologies.	External, multiple sources will likely be required to capture a comprehensive picture of abusive activity in the DNS. Possible sources include the Anti-Phishing Working Group, Surbl, Spamhaus and others.	Trust
1.16	Quantity and relative incidence of fraudulent transactions caused by phishing sites in new gTLDs.		Trust
1.17	Quantity and relative incidence of detected phishing sites using new gTLDs		Trust
1.18	Quantity and relative incidence of detected botnets and malware distributed using new gTLDs.		Trust

1.21	Relative incidence of errors in new gTLD zones.	Internal, technical services team. Will require some clearer definition of "errors."	Trust
2.10	Automated analysis or online survey to determine the number of "duplicate" registrations in new gTLDs. For purposes of this measure, "duplicate" registrations are those where registrant reports having (and still maintaining) the same domain name in a legacy gTLD. Open gTLDs only.	Internal, consumer survey results. 2.10 is related to 2.9 but may require survey results from a statistically significant sample of relevant registrants.	Choice
2.14	DNS traffic in new gTLDs should be compared to contemporary user traffic in legacy gTLDs. DNS traffic is an indicator of trust, choice, and competition. If comprehensive traffic data is not available, sampling should be used.	External, registry reports, DNS traffic market research. Some of the data may be reported by registry operators, while some purchased data may be required for a more complete picture.	Choice
3.7	To assess competitive impact of new gTLDs, measure the quantity of second level registrations per gTLD and ccTLD on a weekly or other interval. TLD attributes should be noted with the data (i.e. open TLDs, closed keyword TLDs, registration, country of operations, single registrant, etc.).	Internal, external, zone files. While gTLD zone file data is readily available, ccTLD data is not or may have use restrictions. This may limit the review team's ability to comprehensively analyze the data.	Competition
5.2	Growth in use of hosted pages for organizations (such as Facebook or Google+)	External, market research. May want to consider in parallel with survey metrics related to use of tools that hide URLs.	Trust
5.3	Growth in use of QR codes		Trust
5.4	Growth in use of URL shortening services		Trust
5.5	Growth in registrations in ccTLDs relative to gTLDs	Internal, technical services team. Will require data from ccTLDs, which may not provide a representative sample. In addition, ccTLD data may have use restrictions.	Trust
6.2	Number of complaints to police agencies alleging fraud or misrepresentation based on – or traced to – domain names	External, fraud reports, government and law enforcement authorities. May be difficult to gather a representative sample of data that can be traced to domain names. May have to rely on reports more generally tracking cyber crime.	Trust

Metric	Description	Data source/considerations	Category
1.5	% Uptime for Registrar services such as WHOIS, contact info, and complaints, assuming that SLAs are established for these measures in the new RAA.	Internal, technical services and RAAs, dependent upon established SLAs	Trust
1.11	Quantity of intellectual property claims and cost of domain name policing relating to new gTLDs. Relative incidence of IP claims made in good faith should be measured in 3 areas: IP claims against registrants regarding second level domains in new gLTDs; IP claims against registrars regarding Second level domains in new gTLDs; IP claims against new gTLD registries regarding second level domains and TLDs. Quantity of second level domains acquired because of infringement or other violations of IP rights of acquiring parties; and Cost of domain name policing and enforcement efforts by IP owners.	External, IAG-CCT members exploring feasibility with International Trademark Association (INTA,) which has expressed an interesting in polling their members on this topic. Subject to some definition of terms, such as which costs would be included, whether these are internal or external (in-house vs. outside counsel.)	Trust
1.13	Quantity of Compliance Concerns regarding Applicable National Laws, including reported data security breaches.	Internal, compliance team. Data security breaches are tracked, but not concerns related to applicable national laws. Rephrased to read: Quantity of compliance concerns regarding data security breaches.	Trust
1.14	Quantity and relative incidence of domain takedowns.	External, will require reporting from registries	Trust
1.15	Quantity and relative incidence of spam from domains in new gTLDs, which could be measured via specialized email addresses and methodologies.	External, multiple sources will likely be required to capture a comprehensive picture of abusive activity in the DNS. Possible sources include the Anti-Phishing Working Group, Surbl, Spamhaus and others.	Trust
1.16	Quantity and relative incidence of fraudulent transactions caused by phishing sites in new gTLDs.	See 1.15.	Trust
1.17	Quantity and relative incidence of detected phishing sites using new gTLDs	See 1.15.	Trust

1.18	Quantity and relative incidence of detected botnets and malware distributed using new gTLDs.	See 1.15.	Trust
1.21	Relative incidence of errors in new gTLD zones.	Internal, technical services team. Will require some clearer definition of “errors.”	Trust
2.8	Measure share of Sunrise registrations & domain blocks to total registrations in each new gTLD.	Internal, may require some data from registries.	Choice
2.9	Relative share of new gTLD registrations already having the same domain in legacy TLDs prior to expansion. For this measure, count all registrations that redirect to domains in legacy TLDs. Open gTLDs only.	Internal, technical services team. The team can query redirects in the system to SLDs that match between legacy TLDs and new gTLDs.	Choice
2.10	Automated analysis or online survey to determine the number of “duplicate” registrations in new gTLDs. For purposes of this measure, "duplicate" registrations are those where registrant reports having (and still maintaining) the same domain name in a legacy gTLD. Open gTLDs only.	Internal, consumer survey results. 2.10 is related to 2.9 but may require survey results from a statistically significant sample of relevant registrants.	Choice
2.14	DNS traffic in new gTLDs should be compared to contemporary user traffic in legacy gTLDs. DNS traffic is an indicator of trust, choice, and competition. If comprehensive traffic data is not available, sampling should be used.	External, registry reports, DNS traffic market research. Some of the data may be reported by registry operators, while some purchased data may be required for a more complete picture.	Choice
3.7	To assess competitive impact of new gTLDs, measure the quantity of second level registrations per gTLD and ccTLD on a weekly or other interval. TLD attributes should be noted with the data (i.e. open TLDs, closed keyword TLDs, registration, country of operations, single registrant, etc.).	Internal, external, zone files. While gTLD zone file data is readily available, ccTLD data is not or may have use restrictions. This may limit the review team’s ability to comprehensively analyze the data.	Competition
3.8	Quantity of “unique” second level registrations in the new gTLD space where that same string does not appear as a registration in any other TLD on a weekly or other interval basis (data analyzed in conjunction with website traffic identified in metric 2.14). Open gTLDs only.	See 2.14 and 3.7.	Competition

4.4	Frequency of dead-end domains (registered but do not resolve)	Internal, technical services team. May require comparing zone files to Whois records.	Trust
4.5	Numbers of complaints received by ICANN regarding improper use of domains	Internal, compliance team. Will require defining “improper use” with categories of compliance categories already tracked in system.	Trust
5.2	Growth in use of hosted pages for organizations (such as Facebook or Google+)	External, market research. May want to consider in parallel with survey metrics related to use of tools that hide URLs.	Trust
5.3	Growth in use of QR codes	See 5.2.	Trust
5.4	Growth in use of URL shortening services	See 5.2.	Trust
5.5	Growth in registrations in ccTLDs relative to gTLDs	Internal, technical services team. Will require data from ccTLDs, which may not provide a representative sample. In addition, ccTLD data may have use restrictions.	Trust
6.2	Number of complaints to police agencies alleging fraud or misrepresentation based on – or traced to – domain names	External, fraud reports, government and law enforcement authorities. May be difficult to gather a representative sample of data that can be traced to domain names. May have to rely on reports more generally tracking cyber crime.	Trust