OWNERS: Laureen (lead), Carlos, Calvin

Refer to Laureen's Model Issue Paper -
https://docs.google.com/document/d/1rswTUNmvB_Lkt2RDwU2OuNx13pptdP_TpgCZ3V77UBk/edit?usp=sharing

HIGH LEVEL QUESTION: Have the safeguards been fully implemented? *[focus on GAC Safeguards Beijing and beyond; Calvin/Carlos to focus on technical safeguards; David's teams to focus on RPM implementation].*

OWNER: Laureen Kapin

SUB-QUESTIONS:

1. Have the safeguards applicable to all new gTLDs been fully implemented?
    a. WHOIS verification and checks and of same (directed to Registry operators)
    b. Mitigating abusive activity (directed to Registry Operators)
    c. Security checks
    d. Documentation (inaccurate WHOIS and security threats)
    e. Making and Handling Complaints
    f. Consequences

2. Have the safeguards applicable to ~~(~~new~~)~~ gTLDs that raise consumer protection concerns, contain sensitive strings, or contain strings in regulated markets been fully implemented? **Note: GAC directed responsibility for these safeguards to Registry Operators.**
    a. Compliance with applicable laws (Registry Operators include in acceptable use policy that Registrants comply w/all applicable laws; Registry Operators require Registrars to notify Registrants of this requirement at time of registration)
    b. Implement reasonable/appropriate security measures for collection of sensitive financial/health information
    c. Establish relationship with relevant regulatory/industry bodies to mitigate risks of illegal activity
    d. Require Registrants to have a single point of contact for complaint reporting and contact info for relevant regulatory bodies

Formatted: Left

Formatted: List Paragraph, Indent: First line: 0"

3. Have the safeguards applicable to highly regulated gTLDs been fully implanted?
    a. Verify/validate credentials
        i. In case of doubt, consult with relevant authorities
        ii. conduct periodic post-– registration checks to ensure registrants' validity

4. Safeguards for gTLDs with inherent gov't functions (.army .navy; .airforce)?

5. Safeguards for gTLDs that may have increased risk of cyber bullying/harassment?
    a. Develop clear policies to minimize risks of cyber bullying/harassment

6. Have the safeguards applicable to restricted registration policies been fully implemented? [perhaps also a Competition issue?]
    a. Ensure registration restrictions appropriate for risks associated with particular gTLDs
    b. Ensure registration restrictions are transparent
    c. Ensure registration restrictions do not result in either an undue preference or an undue disadvantage to registrars and registrants

FINDINGS: Generally speaking, many GAC safeguards applicable to new gTLDs have been implemented via contract provisions in the standard (2013) Registry and Registrar Agreements required for all new gTLDs. However, certain aspects of GAC advice were not implemented as advised and certain important safeguards have not been implemented at all. Whether the safeguards as implemented have been effective, or have been effectively enforced are separate questions.

1. Only certain safeguards applicable to all new gTLDs have been fully implemented as advised.
    a. WHOIS verification and checks and of same/ **Modified implementation:** ICANN (not the Registry Operators) to undertake the checks at least twice annually. Will report inaccurate WHOIS records to Registrars for follow-up and feedback on the outcome to the ICANN Compliance.

    b. Mitigating abusive activity/ **Modified Implementation:** via Public Interest Commitments in Specification 11, ¶3a (PICs in Spec.11). Responsibility delegated from Registry Operators to the Registrars via Registry-Registrar Agreement document and downstream contracts with registrants.

Formatted: Indent: Before: 0", First line: 0"
Formatted: Indent: Before: 0.5"
Formatted: Highlight
Formatted: Indent: Before: 1.5"
Formatted: Indent: Before: 2.25"
Formatted: Indent: Before: 0.5"
Formatted: Indent: Before: 1.5"
Formatted: Indent: Before: 0.75"
Formatted: Indent: Before: 1.5"
Formatted: Indent: Before: 0"
Formatted: Font: Bold
Formatted: Indent: Before: 0"

c. Security checks/ **Not implemented as intended:** Spec 11, ¶ 3b requires security checks. However**,** GAC advice included enforcement mechanism calling for Registry Operator to notify Registrar if detected threats pose an actual risk of harm and provides for suspension domain name until matter is resolved if Registrar fails to act. The modified implementation undermines ¶3a as well because although the abusive activity is prohibited; the corresponding steps stop at detection, with no duty to notify or take further action. **Note: Discussions on how to implement the Spec. 11 security checks framework are currently underway.**

d. Documentation (inaccurate WHOIS and security threats)/ **Partial implementation:** for maintaining reports of security threats, implemented via PICs in Spec 11, ¶3; for inaccurate WHOIS information, see WHOIS Accuracy Reporting System (ARS). GAC advised Registry Operators to maintain statistical reports of inaccurate WHOIS records. ARS is an ICANN project taken in part to respond to this GAC safeguard requiring documentation of WHOIS inaccuracies. This implementation shifted responsibility from Registry Operators to ICANN. Further, the ICANN ARS has only dealt with accuracy of syntax and operability (i.e., is the contact information in the correct format and is it an operating email, address or phone number). There is not a commitment to progressing to the identity validation phase (i.e., is the individual listed responsible for the domain?). The identity validation phase is crucial to confirming the accuracy of the WHOIS record. Hence, this implementation lacks a key component of the intended safeguard.

e. Making and Handling Complaints/ **Implemented** via Section 2.8 and Specification 6, Section 4.1 of the standard Registry Agreement (although GAC has expressed concerns about specifics of implementation; see e.g., Singapore 2014 Communique).

f. Consequences/**Implemented** for domains used in breach of applicable laws: Spec. 11, ¶3a standard Registry Agreement; for false WHOIS: 3.7.7.2 of standard 2013 Registrar Accreditation Agreement. Both provisions include suspension as a possible consequence. However, query whether the PIC provision as written provides "real and immediate" consequences especially in light of complex and lengthy PIC DRP.

Sources: Beijing Communique; GAC Advice Effectiveness Review; Singapore 2014 Communique; Los Angeles 2014 Communique; London Communique; January 9, 2014 Registry Agreement (standard Registry Agreement), WHOIS Accuracy Reporting System https://whois.icann.org/en/whoisars;
[consider adding other Communiques; GAC/Board correspondence (including July 3, 2013 and other scorecards); and stakeholder correspondence]

2. Safeguards applicable to gTLDs that raise consumer protection concerns, contain sensitive strings, or contain strings in regulated markets have generally not been fully implemented. **Note: GAC directed responsibility for these safeguards to Registry Operators.**
   a. Compliance with applicable laws (Registry Operators include in acceptable use policy that Registrants comply w/all applicable laws; Registry Operators require Registrars to notify Registrants of this requirement at time of registration)/**Partially implemented via Spec 11, ¶3a.**
   b. Implement reasonable/appropriate security measures for collection of sensitive financial/health information/**Not implemented**
   c. Establish relationship with relevant regulatory/industry bodies to mitigate risks of illegal activity/**Not implemented**

d. Require Registrants to have a single point of contact for complaint reporting and contact info for relevant regulatory bodies/**Not Implemented**

Sources: Beijing Communique; GAC Advice Effectiveness Review; January 9, 2014 Registry Agreement (standard Registry Agreement), ICANN Implementation Framework for GAC Category 1 Implementation Advice https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf, [consider adding other Communiques; GAC/Board correspondence (including Oct. 29, 2013 and other scorecards); and stakeholder correspondence]

3. Safeguards applicable to highly regulated gTLDs have not been implemented as advised.
    a. **Board did not implement** GAC advice: Verify/validate credentials
        i. In case of doubt, consult with relevant authorities
        ii. conduct periodic post-registration checks to ensure registrants' validity

    b. **NGPC modifies GAC advice** about requirement of "verification" and "validation" of licenses, credential, etc. to a requiring a "representation" from registrant that they have the necessary authorizations, charters, licenses, etc. (¶ 6). Registry Operators are only required to consult with authorities re: licensing or the like, if a complaint is received. (¶ 7). Registrants self-report any "material changes" re: their credentials. (¶ 8).

    Sources: Beijing Communique; Los Angeles Communique; London Communique; GAC Advice Effectiveness Review; January 9, 2014 Registry Agreement (standard Registry Agreement), ICANN Implementation Framework for GAC Category 1 Implementation Advice https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf
    [consider adding other Communiques; GAC/Board correspondence (including Oct. 29, 2013 and other scorecards); and stakeholder correspondence]

4. Safeguards for gTLDs with inherent gov't functions (.army .navy; .airforce). **Implemented:** Registry operator will include a provision in its Registry---Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring a representation that the Registrant will take reasonable steps to avoid misrepresenting or falsely implying that the Registrant or its business is affiliated with, sponsored or endorsed by one or more country's or government's military forces if such affiliation, sponsorship or endorsement does not exist.

    Sources: Beijing Communique; ICANN Implementation Framework for GAC Category 1 Implementation Advice https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf

5. Safeguards for gTLDs that may have increased risk of cyber bullying/harassment/ **Implemented:** Registry Operator will develop and publish registration policies to minimize the risk of cyber bullying and/or harassment for specified strings.

Sources: Beijing Communique; GAC Advice Effectiveness Review; January 9, 2014 Registry Agreement (standard Registry Agreement), ICANN Implementation Framework for GAC Category 1 Implementation Advice https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf

6. Safeguards applicable to restricted registration policies. [perhaps also a Competition issue?] **Partially implemented.** GAC advice reflects ongoing concerns about whether restricted registration policies lead to undue preferences.
    a. Ensure registration restrictions appropriate for risks associated with particular gTLDs
    b. Ensure registration restrictions are transparent
    c. Ensure registration restrictions do not result in either an undue preference or an undue disadvantage to registrars and registrants

Sources: Beijing Communique; GAC Advice Effectiveness Review; January 9, 2014 Registry Agreement (standard Registry Agreement), ICANN Implementation Framework for GAC Category 1 Implementation Advice https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf; Singapore 2014 Communique; Los Angeles 2014 Communique; London Communique; consider adding other Communiques and correspondence

Possible CAUSES:

1. ~~1.~~ GAC joined by certain other constituencies within the multistakeholder community pressed for meaningful implementation of the GAC Safeguards.

GAC safeguard advice issued somewhat late in the negotiating process of the new standard Registry and Registrar Agreements. .

2. Safeguards also generated some controversy and disagreements about whether and to what extent they could/should be implemented. See NGPC correspondence re: rationale for changes.
3. Certain stakeholder groups have raised concerns about practical ability to implement GAC advice and increased costs resulting from implementation of certain safeguards and may suggest revisiting already implemented safeguards while other stakeholder groups have raised concerns that the safeguards have not been sufficiently implemented and/or enforced.
4. The GAC Advice was added in the very last minute and early months of 2013 to the ongoing revision of the RAA. Staff put a lot of pressure on GAC to finish the advice so it could be inlcude~~3~~d in the first RAA contracts to be signed in April 2013. Maybe there was not enough time for GAC and community to ~~ot~~ revise and comment on the final draft of the specs 11 section of the 2013 RAA, which in the end is only subject of a bilateral negotiations between ICANN the Corporation and the signatories (or new applicants)

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

PRIORITY TO ADDRESS: High priority and should be addressed prior to subsequent rounds so that applicants are aware of what they will need to comply with in advance of submitting an application for a new gTLD.

RECOMMENDATIONS:

1. Consider whether there has been sufficient implementation of safeguards.
    a. Consider whether to gather data on ~~Does the impact of the new safeguards have been adequately considered in terms of the~~ whether implementation of the new Safeguards increased compliance responsibilities (in terms of ICANN~~,~~ budget and resources) ~~organizational structure of ICANN~~?
    ~~Is the compliance function adequately addressing the safeguards issues that have aroused so far?a.~~
    b. For safeguards that have not been adequately implemented, consider whether they should be implemented/refined based upon consumer expectations, particularly those that relate to expectations about registration restrictions and concerns about the online security of sensitive health and financial information [see Nielsen and NCC data]; also weigh against cost/benefits of implementing advice and practical challenges of implementation
        i. Board/Staff recommendation
        ii. Likely requires research data (particularly to gather additional information on reasons for increase or decrease in perceived trustworthiness)

2. Consider restrictions on who can purchase gTLDs to ensure that user expectations are met regarding: a. relationship of content of gTLD to name of gTLD and b. implied messages of trust conveyed by names of gTLDs (particularly in sensitive or regulated industries as advised by GAC)

    a. Board/Staff recommendation
    b. Would require changes in standard contracts and could increase compliance costs

REVIEW:

1. Consider collecting data comparing trustworthiness of new gTLDs with restrictions on registration to new gTLDs with few or no restrictions.
2. Cost/benefits of compliance Consider how to weigh cost/benefits of safeguard implementation (for example for verification/validation could look to those new gTLDs that have voluntarily included verification/validation requirements)
3. Repeat selected parts of Nielsen study and look for increase in perceived trustworthiness of new gTLDs and seek data on reasons for increase or decrease
4. Review in two years to assess and recommend changes if an increase in trust is not observed.

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1"

Formatted: Font: (Default) Times New Roman, (Asian) Times New Roman, 7 pt, Complex Script Font: Times New Roman, 7 pt

Formatted: Font: (Default) Times New Roman, (Asian) Times New Roman, 7 pt, Complex Script Font: Times New Roman, 7 pt

Formatted: Font: 12 pt, Complex Script Font: 12 pt

Formatted: Font: 12 pt, Complex Script Font: 12 pt

Formatted: Font: 24 pt, Complex Script Font: 24 pt

#4 Segment on Technical safeguards

Formatted: Left

Formatted: Font: 24 pt, Complex Script Font: 24 pt

CCT-RT DISCUSSION PAPER WORKSHEET

HIGH LEVEL QUESTION: Have the safeguards been fully implemented? *[Calvin/Carlos to focus on technical safeguards].*

OWNER: Calvin Browne

SUB-QUESTIONS:

1. Have the Technical safeguards applicable to all new gTLDs been fully implemented?
    a. Have registry operators been technically vetted.
    b. Has DNSSEC been deployed (and monitored).
    c. Has Wild-carding been prevented.
    d. Has orphan glue been appropriately managed.
    e. Has Thick WHOIS been implemented.
    f. Has centralized access to zone file data been implemented.
    g. Expedited Registry Security Request (ERSR) Process.
    h. Voluntary framework for high-security zones/High security top-level domain-draft program development.

FINDINGS: Generally speaking, most Technical safeguards applicable to new gTLDs have been implemented via contract provisions in the standard Registry and Registrar Agreements required for all new gTLDs. Additionally, before delegation can take place, passing of Pre-Delegation Testing (PDT) is mandatory for all GTLDs Whether the safeguards as implemented have been effective, or have been effectively enforced are separate questions.

1.

a. As a requirement in the application process, all nGTLD applicants had to provide a full description of technical back end services, even where subcontracted. This was a first cut at ensuring technical competence. These provided technical descriptions were evaluated at application time. It would make little sense to audit registry operators against these initial applications on an on-going basis as technical requirements change. Additionally, all applicants were required to pass Pre-Delegation Testing (PDT). PDT included comprehensive technical checks of EPP, Name Server setup, DNSSEC etc. Passing of these tests was an absolute requirement in order to get Delegation of a domain.

b. DNSSEC is an absolute contractual requirement. Additionally, DNSSEC is actively monitored and compliance notices raised if and when checks fail. See ICANN Registry agreement (https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm) specification 6, clause 1.3.

c. Wild-carding is absolutely prevented by contract. Given the nature of wild-carding, it is not possible to monitor this on an ongoing basis, but given the nature of wild-carding, it stands to reason that a registry deploying wild-carding would quickly be found out. See ICANN Registry agreement specification 6, clause 2.2.

d. It is a Contractual requirement for the registry to remove orphan glue, when presented of evidence of such glue used in malicious conduct. See ICANN Registry agreement specification 6, clause 4.1. Anecdotally, some registries have implemented registration policies that make this a non-issue with orphan glue records being technically prevented by registration policies.

e. Thick WHOIS is an absolute contractual requirement. Additionally, ICANN compliance monitors this on an active basis, for both reachability and format. Accuracy of WHOIS is a different matter and a different process applies to this. See ICANN Registry agreement specification 10, Section 4

f. Again, it is a contractual requirement that a registry makes their zone files available. ICANN has implemented Centralized Zone Data Service (https://czds.icann.org/en) in order for registries to comply with this. See ICANN Registry agreement specification 4, section 2.1.

g. The ERSR process https://www.icann.org/resources/pages/ersr-2012-02-25-en "has been developed to provide a process for gTLD registries who inform ICANN of a present or imminent security incident (hereinafter referred to as "Incident") to their TLD and/or the DNS to request a

contractual waiver for actions it might take or has taken to mitigate or eliminate an Incident". [need to see if and if so, how many times this has been activated]

h. These two concepts appear to be two ideas raised in the formation of the nGLTD program that appear not to have progressed to implementation. They appear to be a voluntary idea for a type of nGTLD that would require extra security/authentication for registration purposes. Neither concept appears to have moved from a draft idea. [do we want to explore this further – idea appears stillborn due to lack of consensus/difficulty to agree on implementation]

CAUSES:

1. GAC jd.

PRIORITY TO ADDRESS: High priority and should be addressed prior to subsequent rounds so that applicants are aware of what they will need to comply with in advance of submitting an application for a new gTLD.

RECOMMENDATIONS:

1. Consider whether there has been sufficient implementation of safeguards.
    a. For safeguards that have not been implemented, consider whether they should be implemented based upon consumer expectations [see Nielsen data]; also weigh against cost/benefits of implementing advice and practical challenges of implementation
        i. Board/Staff recommendation
        ii. Likely requires research data

2. Consider restrictions on who can purchase gTLDs to ensure that user expectations are met regarding: a. relationship of content of gTLD to name of gTLD and b. implied messages of trust conveyed by names of gTLDs (particularly in sensitive or regulated industries as advised by GAC)

    a. Board/Staff recommendation
    b. Would require changes in standard contracts and could increase compliance costs

REVIEW:

1. Consider collecting data comparing trustworthiness of new gTLDs with restrictions on registration to new gTLDs with few or no restrictions.
2. Consider how to weigh cost/benefits of safeguard implementation (for example for verification/validation could look to those new gTLDs that have voluntarily included verification/validation requirements)
3. Repeat selected parts of Nielsen study and look for increase in perceived trustworthiness of new gTLDs

4. Review in two years to assess and recommend changes if an increase in trust is not observed.