## Consumer Trust and Safeguards Draft Findings

1. Has the new gTLD program put mechanisms in place to improve trustworthiness of the DNS?
    i. Yes, new gTLD program included numerous safeguards that were incorporated into Registry Agreements and downstream agreements Registrar Agreements and Registrar Registrant Agreements. These are contract obligation subject to ICANN Compliance procedures.

b. Safeguards/Have the Safeguards for New gTLDs Been Implemented?

i. Technical Safeguards

- 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 new GTLDs.
- Technical Safeguards Implemented:
    - Technically vetted applicants
    - DNSSEC deployed (and monitored)
    - Wild-carding prevented.
    - Orphan glue appropriately managed
    - Thick WHOIS
    - Centralized access to zone file data
    - Expedited Registry Security Request (ERSR) Process **[As of October 5, 2016, this process had not been invoked for a new gTLD]**
- Technical Safeguards Not Implemented:
    - Voluntary framework for high-security zones/High security top level domain-draft program development **[not implemented]**

ii. Safeguards Applicable to all New gTLDs Implemented:

- WHOIS verification and documentation and checks and of same
- Mitigating abusive activity (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) consequences for such activities including suspension of the domain name)
- Security checks (conduct 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)

- Procedures for Making and Handling Complaints; Abuse Contact

iii. Safeguards Applicable to New gTLDs that Raise Consumer Protection Concerns, Contain Sensitive Strings, or Contain Strings in Regulated Markets Implemented:
   - Compliance with applicable laws (provision requiring registrants to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct, fair lending, debt collection, organic farming, disclosure of data, and financial disclosures)
   - Implement reasonable/appropriate security measures for collection of sensitive financial/health information

iv. Safeguards Applicable to New gTLDs that Raise Consumer Protection Concerns, Contain Sensitive Strings, or Contain Strings in Highly Regulated Markets
   - Establish relationship with relevant regulatory/industry bodies to mitigate risks of illegal activity:
   - Require Registrants to have a single point of contact for complaint reporting and contact info for relevant regulatory bodies:
   - Verification/validation of credentials: Representation that the Registrant possesses any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string.
      - Duty to consult if Complaint (If Registry Operator receives complaint re: authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents regarding the authenticity)
      - Duty to Update Credential Status (Registrant)

c. Voluntary Public Interest Commitments
   - Domains could choose to incorporate additional, voluntary Public Interest Commitments into their Registry Agreements.
      - These would generally consist of incorporating statements made as part of their application into Specification 11, Section 2 of their Registry Agreement; electing to include other voluntary PICs under Specification 11, Section 4; or including additional commitments under Specification 12, Community Registration Policies
   - ICANN's new gTLD status website indicates that 513 applicants submitted voluntary public interest commitments (the applications predated the subsequent distinction ICANN developed between mandatory and voluntary PICs)
   - 71 out of 116 regulated gTLDs adopted voluntary PICs
   - 17 out of 29 highly regulated gTLDs adopted voluntary PICs

d. Rights Protection Mechanisms

2. Has the new gTLD Program Put Sufficient Mechanisms in Place to Mitigate Risks to the Trustworthiness of the DNS?
    a. Have the Safeguards Been Implemented in a Manner that Promotes Effective Enforcement? [combine Calvin, LK and Carlton]
        i. Technical Safeguards **[Calvin? Thoughts on this topic?]**
        ii. Safeguards Applicable to all New gTLDs that raise enforcement issues:
            - WHOIS: language of the WHOIS contract provisions specifies clear obligations and timelines
                - ICANN itself implemented a WHOIS Accuracy Reporting System (ARS).
                - Current ARS system measures accuracy of syntax and operability
                - ICANN does not require identity validation either via the new gTLD contracts or through its own ARS
            - Security Checks: The obligation to engage in security checks can be enforced, as implemented. Nevertheless, the safeguard lacks obligations on either notification to the Registrar or how to respond to security threats.
                - Community discussions on how to Develop a Framework for Registry Operators to conduct periodic security checks and respond to identified security threats are currently underway. https://myicann.org/plan/project/54398430005f4feb0a04e53e8afaa73b
            - Making/Handling Complaints: The implemented language creates a duty to investigate and respond to complaints from government agencies.
                - The implemented language does not mandate specific mechanisms to investigate and respond to complaints from members of the public
                - GAC has expressed concerns about specifics of implementation; see e.g., Singapore 2014 Communique, particularly what constitutes "reasonable steps" to investigate and respond to complaints
        iii. Safeguards Applicable to New gTLDs that Raise Consumer Protection Concerns, Contain Sensitive Strings, or Contain Strings in Regulated Markets
            - Difficult to assess because ICANN Compliance does not categorize complaints by safeguards (e.g., complaints about compliance with applicable laws and security measures to protect sensitive health and financial information)
        iv. Safeguards Applicable to New gTLDs that Raise Consumer Protection Concerns, Contain Sensitive Strings, or Contain Strings in Highly Regulated Markets
            - Establish relationship with relevant regulatory/industry bodies to mitigate risks of illegal activity: implementation language appears to require only publicizing a point of contact and issuing an invitation rather than actually establishing a working relationship

- *Registry operators will proactively create a clear pathway for the creation of a working relationship with the relevant regulatory or industry self---regulatory bodies by publicizing a point of contact and inviting such bodies to establish a channel of communication. . .*

- Verification/validation of credentials: Advice in GAC Communiqués following this implementation reflects concerns that the advice as implemented may not adequately protect the public:

  - The GAC advice required Registry Operators to proactively screen Category 1 Registrants to ensure that they are what they purport to be before they may do business with the public using the name of a regulated sector such as a bank or pharmacy. The looser requirement that registrants provide some "representation" that they possess the appropriate credentials (e.g. as a bank, insurer, pharmacy, etc.) poses the risk of consumer fraud and potential harm because bad actors will not hesitate to make false representations about their credentials.

b. Voluntary Public Interest Commitments **[TBD awaiting data from interviews]**
   - As of mid-October 2016, ICANN reports receiving no complaints alleging breach of a voluntary PIC
c. Rights Protection Mechanisms **[TBD awaiting data from INTA study]**
d. What was the impact of the new safeguards on DNS Abuse? **[TBD awaiting Data from DNS abuse study]**
   i. Consider whether we want to include data from other sources [Carlton has noted statistics from Spamhaus and the AntiPhishing Working Group in his paper on Effectiveness of Procedures to Enforce safeguards]

## 3. Have these Efforts had an Impact on Public Perception of the DNS?

**a. Do Consumer Trust New gTLDs?**

- Trust appears tied to familiarity and reputation. Familiarity often depends on visitation.
- Consumers visit gTLDs based upon relevance of gTLD to the information they seek.

- Consumers do not trust new gTLDs as much as legacy gTLDs
  1) Consumers do not trust new gTLDs as much as legacy gTLDs
     a. 2015 90% find legacy gTLDs very/somewhat trustworthy compared to 49% for new gTLDs
     b. 2016 91% find legacy gTLDs very/somewhat trustworthy compared to 45% for new gTLDs (52% for added gTLDs)

- Registrants perceive certain new gTLDs as trustworthy but not as trustworthy as legacy gTLDs

2) When asked about specified gTLDs, Registrants perception of certain new gTLDs as "trustworthy" increased from 58% to 60% over 2015-2016.

3) Registrants, however, associate the term "trustworthy" more with legacy gTLDs than new gTLDs:
    a. 2015 83% legacy vs. 58% new gTLDs
    b. 2016 79% legacy vs. 60% new gTLDs

- Consumer's willingness (comfort level) to provide sensitive information is about half as much for new gTLDs compared to legacy gTLDs.

4) Do consumers feel "somewhat comfortable providing sensitive information to new gTLDs compared to legacy gTLDs?
    a. Home address:
        i. .com 83%
        ii. New gTLD 44%

    b. Financial info:
        i. .com 62%
        ii. New gTLD 36%

    c. Healthcare info:
        i. .com 68%
        ii. New gTLD 40%

- Restrictions on who can purchase domain names contribute to consumer/registrant trust and both groups expect restrictions and trust that restrictions will be enforced.
- Reputation and Familiarity are key factors that make domain extensions trustworthy
- Security concerns and lack of familiarity may lead the public to avoid certain domains.

**b. Are Consumers Aware of New gTLDs?**

- Consumer awareness of new gTLDs increased from 46% to 62% **[verify could be 52% pg. 8 vs. pg. 42]** between 2015-16
- Registrant total awareness of new gTLDs showed small decrease in 2016 to 64% from 66% in 2015 (average awareness of specified gTLDs is lower (2016: 20%  2015 22%; but added new gTLDs: 2016: 25%)

**c. Has Consumer Trust in the DNS Improved Overall Since the Introduction of New gTLDs?**

- 2015: Half of consumers trust the Domain Name industry just as much as other tech industries
- 2016: Trust levels remained the same (global total seemed to improved but b/c increase less than 4 percentage points, not possible to say that it actually improved)

- Reputation was the factor most cited as the reason consumers trust the DNS more than other tech industries (also the reason consumers trust the DNS less than other industries)
- Registrants show similar results (2015: 49%; 2016 47%  trust DN industry much more/somewhat more than other industries: ISP's, software co's, computer hardware co's, e-commerce co's and web-based marketing co's)
- For Registrants, reputation and self interest drive trust. Registrants expect industry to follow practices that protect its interests (e.g., security protocols). Those who trust less cite poor security, regulations, and lack of transparency regarding business practices.
- At the very least, trust does not appear to have decreased