OWNER: Laureen Have Safeguards Been Implemented Effectively?
[Other related papers: Calvin to discuss technical safeguards; David to discuss RPMs].

HIGH LEVEL QUESTION: Have the Safeguards Been Implemented In a Manner that Promotes Effective Enforcement?

OWNER: Laureen Kapin

In this paper, the term "safeguards" refers to the safeguards implemented by the ICANN Board in response to advice issued by the Governmental Advisory Committee in the Beijing Communiqué. See https://gacweb.icann.org/display/GACADV/2013-04-11-Safeguards-1

SUB-QUESTIONS: **I) What are the implemented safeguards? II) What was the intended goal of the safeguard?** (Note: the topic of whether safeguards met their intended goals will be discussed in other papers) **III) Have the Safeguards Been Implemented in a Manner that Promotes Effective Enforcement?**

In its Beijing Communiqué, the GAC advised that its safeguards be subject to contractual oversight by ICANN. Generally speaking, many GAC advised safeguards applicable to new gTLDs were implemented via contract provisions in the standard Registry and Registrar Agreements required for all new gTLDs. However, certain aspects of GAC advice were implemented differently than advised. What follows is a discussion of certain key safeguards, focusing on the ability of the safeguard to be enforced via ICANN Contract Compliance and/or individual complaints and/or challenges to potential ~~enforcement~~redress of.

1. **What are the implemented safeguards applicable to all new gTLDs? [see https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-i-agenda-2b-25jun13-en.pdf]**

   Findings:
   a. **Safeguard: WHOIS verification and documentation and checks and of same:**
      - Registrar shall comply with the obligations specified in the Whois Accuracy Program Specification. In addition, notwithstanding anything in the Whois Accuracy Program Specification to the contrary, Registrar shall abide by any

Commented [C1]: I have a problem with the safeguards that pre-date the new gTLD and safeguards developed explicitly for the new gTLD applications. I think it should be worthwhile to make this difference explicit. The WHOIS has its own AoC review, suggestions to improve ti predate the new gTLDs. In the case of abusive parties and malicious conduct I´m not sure if it all started with the new gTLDs or if it predates it. I suggest to have at least two separate sections 1. How the new gTLDs helped to solve old problems, and 2. How the new gTLDs created new ones.

Commented [C2]: Please lets have some time to discuss if we want to address the thorny issue of the lack of a definition of public interest……

Consensus Policy requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy. **Registrar Accreditation Agreement (June 2013), Section 3.7.8**

- Registrar must also validate required fields (postal address; email address; phone) for proper format and consistency and verify email and p2hone number of registered name holder. **Registrar Accreditation Agreement (June 2013) WHOIS Accuracy Program Specification**

- The Registrar Agreement also obliges Registrars to require Registered Name Holders to provide: accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8. **Registrar Accreditation Agreement (June 2013) Section 3.7.7.1**

- Consequences for willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration include suspension and cancellation. **Registrar Accreditation Agreement (June 2013) Section 3.7.7.2**

- ICANN has also implemented the WHOIS Accuracy Reporting System, in an effort to identify and report on accuracy in a systematic way to improve quality of contact data in the WHOIS. The project aims to:
  - Proactively identify inaccurate gTLD registration data, exploring the use of automated tools
  - Forward potentially inaccurate records to registrars for action
  - Publicly report on the resulting actions to encourage improvement.

See **WHOIS Accuracy Reporting System** https://whois.icann.org/en/whoisars

1) **What was the intended goal of the WHOIS Verification safeguard?** Ensuring more focused efforts on combatting identified abuse. *See* "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

2) Have the WHOIS Safeguards Identified Above Been Implemented in a Manner that Promotes Effective Enforcement?

- The language of the WHOIS contract provisions specifies clear obligations and timelines.
- ICANN contract compliance reports indicate that WHOIS related complaints comprise the largest category of complaints received. For example, in 2014 of the 41,790 total complaints received, 29,857 related to WHOIS (most complained about lack of accuracy) (about 71%). In 2015, of the 48,106 total complaints received, 36,354 related to WHOIS (accuracy) (about 75%).
    - These figures indicate that the WHOIS safeguards created contract obligations that were sufficiently specific to generate complaints subject to the ICANN compliance process. See ICANN CCT Compliance Metrics 2014, 2015.

- In addition, ICANN itself implemented a WHOIS Accuracy Reporting System. The GAC had 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. Originally, the ARS contemplated three phases: syntax accuracy; operability accuracy; and identity validation.
    - To date, 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). The latest ARS Report issued in June 2016 and contains findings on the accuracy of syntax (proper format) and operability (can it be used to communicate) of telephone numbers, postal address, and email address for a sampling of both new and legacy gTLDs. *See* https://whois.icann.org/en/whoisars-reporting **[Question for Brian A: can we draw conclusions about enhanced WHOIS requirements of 2013 RAA? Study was quite dense and challenging to understand.]**

    - ICANN ARS does not commit to progressing to the identity validation phase (i.e., is the individual listed responsible for the domain?). In terms of effective enforcement, this documentation effort will only detect

syntax and operability issues but will not detect and therefore not document inaccurate identity. The ICANN Board did not agree to require registry operators to require registrars to perform identity validation and verification~~The lack of a commitment to progress to the identity validation phase may weaken efforts to meet the goal of combating identified abuse because efforts to document WHOIS inaccuracies related to identity remain incomplete~~.

Sources: Beijing Communique; GAC Advice Effectiveness Review; January 9, 2014 Registry Agreement (standard Registry Agreement), WHOIS Accuracy Reporting System https://whois.icann.org/en/whoisars; ICANN Contract Compliance Annual Reports.

Causation/Rationale:
1) Specific language regarding WHOIS obligations and a detailed WHOIS specification may have promoted more focused efforts on combatting abuse by creating clear obligations and hence promoting the ability to make actionable complaints to ICANN compliance.
2) Concerns about costs may have influenced the current lack of commitment to proceeding with the identity validation phase of the WHOIS Accuracy Reporting System.

Recommendation:
1) Analyze ARS Studies to see whether data exists to determine whether WHOIS accuracy has increased under the 2013 RAA.
2) Analyze ICANN contract compliance complaints to identify the subject matter of the complaints (e.g., complaints about syntax, operability, or identity). Identify other potential data sources of WHOIS complaints (registrars, registries, ISPs etc.) and attempt to obtain anonymized data from these sources. If identity is a significant percentage of complaints, consult with stakeholders to explore ~~commit to~~ proceeding with identity phase of ARS project.

b. **Safeguard: Mitigating abusive activity**
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. **Base Registry Agreement (updated 1/9/2014) Specification 11, 3(a).**

1) **What was the intended goal of the mitigating abusive activity safeguard?** The plain language of the safeguard indicates its goal: to mitigate abusive activity (defined as 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). The safeguard addresses this goal by incorporating a downstream contract requirement from Registries to Registrars to Registrants.

2) **Has the safeguard been implemented in a manner that promotes effective enforcement?**

- In 2014, ICANN's proactive monitoring of this Public Interest Commitment incorporated into Specification 11, 3a of the standard Registry Agreement indicated that 99% of Registry Operators had complied with the obligation to include this language in their Registry-Registrar agreements. *See* 2014 ICANN Contract Compliance Annual Report at p 13.
- ICANN compliance reports indicate it received abuse complaints in 2014 and 2015. *See* Contractual Compliance Annual Reports for 2014 and 2015. Abuse complaints are typically higher for registrars than registries. In 2015, ICANN received 438 abuse complaints related to Registrars. These complaints included both legacy and new gTLDs. ICANN noted that these complaints involved in part, "Registrars not taking reasonable and prompt steps to respond to appropriately to reports of abuse, which at a minimum should be to forward valid complaints to the registrants." 2015 ICANN Contractual Compliance Annual Report. These figures indicate that the Mitigating Abuse Safeguard is the subject of complaints and the ICANN compliance process.
- ICANN Compliance notes its limited role in enforcing this safeguard related to illegal activities on websites:

> ICANN is not a governmental or law enforcement agency and has no law enforcement authority. ICANN is also not a court and is not empowered to resolve disputes when parties disagree over what constitutes illegal activity in multiple countries around the world. Therefore, ICANN relies on governmental regulatory authorities and courts to police illegal activity.

https://www.icann.org/resources/pages/faqs-84-2012-02-25-en#31 (Questions Related to ICANN Contractual Compliance Approach and Process).

- The plain language of the safeguard does not obligate the Registry operator to monitor and enforce this provision beyond requiring the provision in the downstream Registrar–Registrant agreement.

Causation: The safeguard's definition of abuse (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) contemplates activities that are more likely to be conducted by registrants or third parties. As a result, the safeguard operates as a downstream requirement that reaches Registrants via the agreements between Registrars and Registrants. https://features.icann.org/safeguards-applicable-all-new-gtlds

The abusive activities also are typically illegal and ICANN compliance messaging indicates that it views its role as limited to enforcement of whether the Registry included the safeguard provision in its Registry/Registrar provision).

Recommendation:
1) Continue to gather data comparing rates of abuse in domains operating under new Registry Agreement and Registrar Agreements to legacy gTLDs.
2) Determine whether it's possible to draw any conclusions about impact of individual safeguards on rates of abuse (it may only be possible to correlate rates of abuse between new gTLDs and legacy gTLDs because each group operate under separate systems of contracts).
3) Survey registrars to find out whether the safeguard has made a difference in the way they approach combatting abuse.

c. **Security checks:**
- 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. **Base Registry Agreement (updated 1/9/2014) Specification 11, 3(b).**

1) **What was intended goal of the security checks safeguard?** More focused efforts on combatting abuse. *See* Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009 https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

2) **Has the safeguard been implemented in a manner that promotes effective enforcement?**
   - ICANN compliance reports engaging in proactive monitoring of this safeguard and determined for example, that 96% of Registries were conducting security checks as per the contract. ICANN 2014 Contractual Compliance Report at p.13 (2014 Registry Compliance Summary).
   - 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. Bejing Communique.
   - 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

Causation: The NGPC reported community concerns about the timing, cost, and scope of conducting security threats. Hence, the safeguard implementation provided "general guidelines for what registry operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks." (see above for project aimed at developing framework) https://features.icann.org/safeguards-applicable-all-new-gtlds

Recommendations: Once completed, review proposed Registry Operator Framework and assess whether framework is a sufficiently clear, effective, and enforceable mechanism to mitigate abuse by providing for specified actions in response to security threats.

d. **Making and Handling Complaints:**
Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement

and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD.
In responding to such reports, Registry Operator will not be required to take any action in contravention of applicable law.
Base Registry Agreement (updated 1/9/2014), Section 2.8, Protection of Legal Rights of Third Parties

Abuse Contact. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details. **Base Registry Agreement (updated 1/9/2014), Specification 6, Section 4,1, Abuse Mitigation.**

1) **What was the intended goal of the complaints handling safeguards?** Ensuring more focused efforts on combatting identified abuse. See "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

2) **Has the safeguard been implemented in a manner that promotes effective enforcement?**
   - 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 (the GAC advice directed a mechanism to handle to complaints but did not restrict complaints to government agencies). Beijing Communique.
   - Nielsen Consumer survey indicated that the public is unsure of how they would report abuse:
     - 31% overall "don't know" who to report site abuse to
     - 31% overall would report abuse to a consumer protection agency
     - 30% overall would report abuse to local police
     - 24% overall would report abuse to website owner or operator
     - 11% overall would report abuse to ICANN

       Source: Nielsen June 2016 Survey at pp.88, 102

   - The 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).
   - ICANN's 2014 Contractual Compliance report noted that Registry Operators "not publishing the email address and primary contact for reports by mail" and "Registry Operators not responding in a timely matter" were a common

contractual compliance issue regarding publishing abuse contact information (at p. 14). Hence, this safeguard can be the subject of complaints and the ICANN compliance process.

Causation/Rationale: The obligation to have mechanisms to respond to complaints likely assists Registries to investigate and possibly combat abuse and may help protect the public by providing information about harmful practices. Concerns about imposing unreasonable burdens on Registries may have driven the decision to restrict the contract obligation to only handling complaints by government agencies.

Recommendations:

1) Survey Registries to find out the volume of complaints they receive from both the public and government agencies.

2) Assess whether mechanisms to report and handle complaints has led to more focused efforts to combat abuse by surveying Registries to find out what actions they take in response to complaints.

Here we get into the safeguards that developed for new gTLDs ¿?

2. **What are the implemented safeguards applicable to new gTLDs that raise consumer protection concerns, contain sensitive strings, or contain strings in regulated markets? Note:** GAC identified a specific group of Category 1 strings subject to these concerns. ICANN advised that only a subset of the recommended strings would fall within the Category 1 protections and only a subset of the recommended safeguards would apply to the strings in regulated markets. Compare Beijing Communique to https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf.

Findings:

a. **Compliance with applicable laws:**
Registry operators will include a provision in their Registry---Registrar Agreements that requires Registrars to include In their Registration Agreements a 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.

Registry operators will include a provision in their Registry---Registrar Agreements that requires

registrars at the time of registration to notify registrants of the requirement to comply with all applicable laws.

b. **Implement reasonable/appropriate security measures for collection of sensitive financial/health information:** Registry operators will include a provision in their Registry---Registrar Agreements that requires Registrars to include In their Registration Agreements a provision requiring that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

1) What was the intended goal of the safeguards? Safeguards 2a, (Compliance with applicable laws) aims at attempting to mitigate abusive activity. Safeguard 2b aims at protecting the public's sensitive information.

2) Have the safeguards been implemented in a manner that promotes effective enforcement?

- It is difficult to determine whether these safeguards have specifically been the subject of complaints to ICANN contract compliance because the categories of complaints identified in ICANN's Compliance Reports do not reach the level of specificity necessary to precisely track each safeguard.

- ICANN Compliance does report that it proactively monitored compliance with Specification 11, ¶3a that includes language requiring compliance with applicable laws, and determined that there was 99% compliance with this provision. ICANN 2014 Contractual Compliance Report at p.13.

Sources: Beijing Communique; GAC Advice Effectiveness Review; January 9, 2014 Registry Agreement (standard Registry Agreement), ICANN Implementation Framework for GAC Category 1 Implementation Advice, see https://newgtlds.icann.org/en/applicants/gac-advice/cat1-safeguards; and https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf, October 29, 2013 letter Crocker to GAC Chair; September 2, 2014 letter Crocker to GAC Chair.

Causation/Rationale: More precise data on the subject matter of complaints, particularly whether complaints relate to the protection of sensitive health or financial information or what type of law violation is being complained of would assist future review teams in their assessment of these safeguards.

Recommendations:
1) Include more detailed information on subject matter of complaints in ICANN Compliance Reports.

2) Survey Registrars to find out how they are complying with the obligation to provide appropriate security measures for sensitive health and financial information.
3) Follow up survey with audit to assess whether Registrars are sufficiently protecting users sensitive information.

3. **What are the implemented safeguards applicable to new gTLDs that raise consumer protection concerns, contain sensitive strings, or contain strings in *highly regulated* gTLDs? Note:** GAC identified ~~a~~ specific ~~group~~ categories of highly regulated Category 1 strings subject to these concerns. ICANN advised that only a subset of the ~~recommended~~ strings falling in the recommended categories would fall within the highly regulated Category 1 protections. Compare Beijing Communique to https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf.

Findings:

a. **Establish relationship with relevant regulatory/industry bodies to mitigate risks of illegal activity:** 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, including for the purpose of facilitating the development of a strategy to mitigate the risks of fraudulent and other illegal activities.

b. **Require Registrants to have a single point of contact for complaint reporting and contact info for relevant regulatory bodies:** Registry operators will include a provision in their Registry---Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to provide administrative contact information, which must be kept up---to---date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self---regulatory, bodies in their main place of business.

1) **What was the intended goal of the safeguards?** Safeguards 3a (relationship with relevant regulatory/industry bodies); 3b (single point of contact for complaint reporting) both attempt to mitigate abusive activity.

2) **Have the safeguards been implemented in a manner that promotes effective enforcement?**

Commented [JH3]: One of the challenges with implementing the GAC advice arose from the GAC deciding not to identify individual strings subject to its advice but instead to use high-level categories like "financial" or "health." The AGB contemplated the GAC providing advice (and early warnings) on specific strings. An added complication was that not all categories or strings potentially within categories are regulated at all or in the same way across jurisdictions. This made it more challenging for the Board to decide which individual strings represented "highly regulated industries."

Commented [C4]: Who expects registry operators to establish working relationships with national authorities PROACTIVELY??? This is hard to understand. Most activities in this area are based on voluntary industry groups, and not direct relations with national authorities.

- In terms of implementing clear obligations, the implementation language for 3a regarding Registrants establishing a relationship with relevant authorities 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. . .

- It is not clear whether complaints about the complaint contact safeguard, which essentially creates a downstream obligation for Registrants to provide complaint related contact information would come to ICANN compliance.

Commented [C5]: Very good!!!

Causation/Rationale: More information on Registry efforts to establish relationships with relevant regulatory/industry bodies would also assist future review teams to assess the effectiveness of this safeguard. This implementation may reflect the practical challenges involved with mandating a relationship with a third-party organization. Regarding the requirement to provide contact information for complaints, key questions would be how easy it is for the public to find information on a website regarding contact information for communicating complaints both to those responsible for the domain and applicable government agencies or regulatory bodies.

Recommendations:
1) Survey Registries to find out what steps they are taking to establish working relationships with relevant government or industry bodies.
2) Survey Registrants to determine the volume of complaints they are receiving from regulatory bodies and their standard practices to respond to those complaints.
3) Assess a sampling of domain websites to see whether contact information to file complaints is sufficiently easy to find.

c. Verify/validate credentials:

Representation re: credentials: Registry operators will include a provision in their Registry---Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring a representation that the Registrant possesses any necessary authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string.

Duty to consult if Complaint: If a Registry Operator receives a complaint expressing doubt with regard to the 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: Registry operators will include a provision in their Registry---Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to report any material changes to the validity of the Registrants' authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

1) **What was the intended goal of the safeguards regarding the verification/validation of credentials?** To mitigate the higher levels of risks of abuse associated with strings in highly regulated industries, which are likely to invoke a higher level of trust to consumers. *See* Beijing and London Communiques.

2) **Have the safeguards been implemented in a manner that promotes effective enforcement?**

- Safeguards applicable to highly regulated gTLDs have been implemented but in a manner that differs from the GAC advice.
- Board did not implement GAC advice that Registry operators:
    - verify/validate registrant's credentials
    - in case of doubt, consult with relevant authorities
    - conduct periodic post-registration checks to ensure registrants' validity

- NGPC modified GAC advice about requirement of "verification" and "validation" of licenses, credential, etc. to:

Commented [C6]: And who is responsible for the validation???? Registrars I guess.

- requiring Registrars to include a provision in their Registrar/Registrant agreement requiring a "representation" from registrant that they have the necessary authorizations, charters, licenses, etc.
- Registry Operators are only required to consult with authorities re: licensing or the like, if a complaint is received.
- Registrants self-report any "material changes" re: their credentials.

(ICANN Implementation Framework for GAC Category 1 Implementation Advice at ¶¶ 6-8, https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf).

- 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.

  See e.g., GAC London Communiqué at p. 10.

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, October 29, 2013 letter Crocker to GAC Chair; February 4, 2014 letter Assistant Secretary for Communications and Information, Department of Commerce to Steve Crocker, September 2, 2014 letter Crocker to GAC Chair.

- Consumers expect restrictions on who can purchase new gTLDs
- Restrictions on who can purchase new gTLDs contribute to consumer trust

Sources: Nielsen, Phase 1, ICANN Global Consumer Research Study p.9-10, 25-26, 44
Nielsen, Phase 2, ICANN Global Consumer Research Study p.9, 13, 26, 60

2016: Nielsen, Wave 2, ICANN Global Registrant Survey p. 14, 18, 29, 67.

Causation: NGPC concerned about practical ability to implement safeguard as advised because of challenges involved for Registrars in verifying credentials of entities in multiple jurisdictions. *See e.g.* October 29, 2013 correspondence; Sept. 2, 2014 correspondence.

Recommendations:

1) Assess whether restrictions regarding possessing necessary credentials are being enforced by auditing registrars and resellers offering the highly restricted TLDs **(**i.e., can an individual or entity without the proper credentials buy a highly regulated domain?).
2) Determine volume and subject matter of complaints regarding domains in highly regulated industries by seeking more detailed information from ICANN compliance and registrar/resellers of highly regulated domains.
3) Compare rates of abuse between those highly regulated gTLDs who have voluntarily agreed to verify and validate credentials to those highly regulated gTLDs that have not.

4. **What are the implemented safeguards for new gTLDs with inherent gov't functions (.army .navy; .airforce)?**

Findings:

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.

a. **What was the intended goal of the safeguard?** By its terms, to mitigate abuse related to misleading representations of affiliations with the government's military forces.

b. **Has the safeguard been implemented in a manner that promotes effective enforcement?** It is not clear whether failure to comply with this safeguard has generated complaints. In addition, the safeguard does not contain any consequences for failure to comply.

Recommendations:

1. Determine whether complaints for failure to comply with this safeguard has generated complaints.
2. Survey Registries to determine how they enforce this safeguard.

5. **What are the implemented safeguards for new gTLDs that may have increased risk of cyber bullying/harassment?**

Findings:

Registry Operator will develop and publish registration policies to minimize the risk of cyber bullying and/or harassment.

a. **What was the intended goal of the safeguard?** By its terms, to mitigate abuse related to cyber bullying/harassment.

b. **Has the safeguard been implemented in a manner that promotes effective enforcement?** It is not clear whether failure to comply with this safeguard has generated complaints. In addition, the safeguard does not contain consequences for failure to comply.

Recommendations:

1. Determine whether there have been complaints for failure to comply with this safeguard.
2. Survey Registries to determine how they enforce this safeguard.

6. **What are the implemented safeguards applicable to restricted registration policies (Category 2 Safeguard)?**

Findings:

a. Registry Operator will operate the TLD in a transparent manner consistent with general principles of openness and non---discrimination by establishing, publishing and adhering to clear registration policies.

b. Registry Operator of a "Generic String" TLD may not impose eligibility criteria for registering names in the TLD that limit registrations exclusively to a single person or entity and/or that person's or entity's "Affiliates" (as defined in Section 2.9(c) of the Registry Agreement).

This safeguard focuses on promoting competition and has generated significant correspondence between the GAC and the Board. **Perhaps a topic for the Competition sub-team.**

Note: GAC advice reflects ongoing concerns about whether restricted registration policies could lead to undue preferences (GAC had originally advised to ensure that registration restrictions were appropriate for risks associated with particular gTLDs)

Source for 2-6: ANNEX 2 --- ICANN NGPC RESOLUTION NO. 2014.02.05. NG01 https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf and ICANN NGPC Resolution 2013.06.25.NG04 - 2013.06.25.NG05 - 2013.06.205.NG06 https://features.icann.org/category-2-safeguard-advice-re-restricted-and-exclusive-registry-access

REVIEW:

1. Collect data comparing trustworthiness of new gTLDs with restrictions on registration to new gTLDs with few or no restrictions.
2. 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.
3. Repeat/refine upcoming data abuse study to determine whether presence of additional safeguards correlates to decrease in abuse.
4. Collect data weighing cost/benefits of implementing various safeguards, including impact on compliance costs and costs for Registries, Registrars, and Registrants. Could look to existing gTLDs for information (for example for verification/validation could look to those new gTLDs that have voluntarily included verification/validation requirements to get a sense of costs involved).