**DRAFT: Potential RAA Amendments**

3.7 Business Dealings, Including with Registered Name Holders.

3.7.TBD Registrar will include in its Registration Agreement a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, engaging (itself or through a subsidiary, affiliate or related party) in phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and will impose (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

3.7.TBD Registrar will conduct a technical analysis twice per calendar year to assess whether Registered Names it sponsors are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registrar will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks (including, but not limited to, ICANN compliance requests, related audits, and any other obligations under Section 3.15). Registrar will maintain these reports for the term of this Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request. Registrar will use these analyses to identify Registered Name Holders who have perpetuated repeated security threats or other violations of the Registration Agreement and impose (consistent with applicable law and any related procedures) consequences on such Registered Name Holders including suspension or termination of their account(s) with Registrar and using commercially reasonable efforts to prevent the same Registered Name Holders from creating new accounts or otherwise registering any additional Registered Names with Registrar. Registrar also will comply with ICANN mandated compliance obligations to impose consequences on such Registered Name Holders including but not limited to the consequences listed herein.

3.15 Registrar Self-Assessment and Audits. Registrar shall complete and deliver to ICANN on a schedule and in the form specified by ICANN from time to time in consultation with registrars a Registrar self-assessment. Registrar shall complete and deliver to ICANN within twenty (20) days following the end of each calendar year, in a form specified by ICANN a certificate executed by the president, chief executive officer, chief financial officer or chief operating officer (or their equivalents) of Registrar certifying compliance with the terms and conditions of this Agreement, including but not limited to 3.7.TBD and 3.7.TBD. ICANN may from time to time (not to exceed twice per calendar year) conduct, or engage a third party to conduct on its behalf, contractual compliance audits to assess compliance by Registrar with the terms and conditions of this Agreement. Any audits pursuant to this Section 3.15 shall be tailored to achieve the purpose of assessing compliance, and ICANN will (a) give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested by ICANN, and (b) use commercially reasonable efforts to conduct such audit in such a manner as to not unreasonably disrupt the operations of Registrar. As part of such audit and upon request by ICANN, Registrar shall timely provide all responsive documents, data (including unredacted RDDS data) and any other information necessary to demonstrate Registrar's compliance with this Agreement and ensure all necessary agreements are in place to provide such documents and data to ICANN. Upon no less than ten (10) days notice (unless otherwise agreed to by Registrar), ICANN may, as part of any contractual compliance audit, conduct site visits during regular business hours to assess compliance by Registrar with the terms and conditions of this Agreement. ICANN shall not disclose Registrar confidential information gathered through such audits except as required by applicable law, legal proceedings, or as expressly permitted by any Specification or Policy (including ICANN's Documentary Information Disclosure Policy, as such policy may be amended from time to time); provided, however, that, except as required by applicable law or legal proceedings, ICANN shall not release any information that Registrar has marked as, or has otherwise designated in writing to ICANN as, a "confidential trade secret," "confidential commercial information" or "confidential financial information" of Registrar. If any applicable law, legal proceeding or Specification or Policy permits such disclosure, ICANN will provide Registrar no less than fifteen (15) days notice of its intent to disclose such information, unless such notice is prohibited by law or legal proceeding. Such notice shall include to whom and in what manner ICANN plans to disclose such information.

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive and act upon reports of abuse involving Registered Names sponsored by Registrar, including reports of DNS Abuse and Illegal Activity. Registrar shall publish an email address or webform to receive such reports on, or conspicuously and readily accessible from, the home page of Registrar's website and in response to RDDS queries in the Registrar Abuse Contact Email data element field (or in another standardized place that may be designated by ICANN from time to time). Where a webform is used, the webform must: (i) not impose unreasonable rate limits on submissions; (ii) allow users to submit attachments up to a reasonable file size limit; and (iii) send a confirmation of the form submission and content of the report by email to the submitter. Within two (2) business days of receipt of a report of abuse, Registrar shall confirm receipt of the report in writing. For the purposes of this Agreement, “DNS Abuse” means ~~malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section) as those terms are defined in Section 2.1 of SAC115 (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>)~~ any activity that makes, or intends to make, use of domain names, the Domain Name System protocol, or any digital identifiers that are similar in form or function to domain names to carry out deceptive, malicious, or illegal activity.

3.18.2 Within ten (10) calendar days of receipt of a report of abuse, w~~W~~hen Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used or has been used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Such actions might include suspending or terminating the relevant Registered Name(s), as appropriate. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage. Within two (2) business days of conducting such investigation and/or mitigation of the reported abusive behavior, but in no case no later than twelve (12) calendar days from receipt of reported abuse, Registrar shall update the reporter in writing as to the status of the investigation, the Registrar’s findings, and the mitigating measures implemented by the Registrar or, if none, an explanation as to why no mitigating measures were implemented. Where Registrar confirms three (3) or more incidents of abusive behavior perpetrated by the same Registered Name Holder, Registrar will suspend or terminate the Registered Name Holder’s account(s) with Registrar and will use commercially reasonable efforts to prevent the same Registered Name Holder from creating new accounts or otherwise registering any additional Registered Names with Registrar.

3.18.3~~2~~ Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions to mitigate Illegal Activity. Within the same 24 hour period, Registrar shall take reasonable steps to mitigate the reported llegal Activity, including by suspending or terminating the relevant Registered Name(s), as appropriate. Within one (1) business day of conducting such investigation, Registrar shall update the reporter in writing as to the status of the investigation, the Registrar’s findings, and the mitigating measures implemented by Registrar or, if none, an explanation as to why no mitigating measures were implemented. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

3.18.4~~3~~ Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice and in compliance with Sections 3.7 and 3.15 of this Agreement. ICANN shall make available, every six months, via publication on its website, public reports regarding Registrar’s response to abuse reports, aggregated and anonymized as appropriate to protect any personal data of natural persons.

5.5 Termination of Agreement by ICANN. This Agreement may be terminated before its expiration by ICANN in any of the following circumstances:

5.5.1 There was a material misrepresentation, material inaccuracy, or materially misleading statement in Registrar's application for Accreditation or renewal of Accreditation or any material accompanying the application.

5.5.2 Registrar:

5.5.2.1 is convicted of or found by a court of competent jurisdiction of a felony or other serious offense related to financial activities, or is judged or declared by a court of competent jurisdiction or found by ICANN in its sole and reasonable discretion to have:

5.5.2.1.1 committed fraud,

5.5.2.1.2 committed a breach of fiduciary duty, or

5.5.2.1.3 with actual knowledge (or through gross negligence) permitted Illegal Activity in the registration or use of domain names or in the provision to Registrar by any Registered Name Holder of inaccurate Whois information; or

5.5.2.1.4 failed to comply with the terms of an order issued by a court of competent jurisdiction relating to use of domain names sponsored by the Registrar;

or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing; or

5.5.2.2 is disciplined by the government of its domicile for conduct involving dishonesty or misuse of funds of others or domain names it Sponsors for others; or

5.5.2.3 is the subject of a non-interlocutory order issued by a court or arbitral tribunal, in each case of competent jurisdiction, finding that Registrar has, directly or through an Affiliate, committed a specific violation(s) of applicable national law or governmental regulation relating to cybersquatting or its equivalent; or

5.5.2.4 is found by ICANN, based on its review of the findings by a court, arbitral tribunals, or otherwise in its sole and reasonable discretion, to have been engaged, either directly or through its Affiliate, in a pattern and practice of trafficking in or use of domain names identical or confusingly similar to a trademark or service mark of a third party in which the Registered Name Holder has no rights or legitimate interest, which trademarks have been registered and used in bad faith~~.~~: or

5.5.2.5 is found by ICANN, based on its review of Registrar’s responses to abuse reports, to have not acted reasonably to mitigate DNS Abuse reported under 3.18 in a timely manner.

5.5.3 Registrar knowingly employs any officer that is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) days of Registrar's knowledge of the foregoing; or any member of Registrar's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registrar's board of directors or similar governing body within thirty (30) days of Registrar's knowledge of the foregoing.

5.5.4 Registrar fails to cure any breach of this Agreement within twenty-one (21) days after ICANN gives Registrar notice of the breach.

5.5.5 Registrar fails to comply with a ruling granting specific performance under Sections 5.7 or 7.1.

5.5.6 Registrar has been in fundamental and material breach of its obligations under this Agreement at least three (3) times within a twelve (12) month period.

5.5.7 Registrar continues acting in a manner that ICANN has reasonably determined endangers the stability or operational integrity of the Internet after receiving three (3) days notice of that determination.

5.5.8 (i) Registrar makes an assignment for the benefit of creditors or similar act; (ii) attachment, garnishment or similar proceedings are commenced against Registrar, which proceedings are a material threat to Registrar's ability to provide Registrar Services for gTLDs, and are not dismissed within sixty (60) days of their commencement; (iii) a trustee, receiver, liquidator or equivalent is appointed in place of Registrar or maintains control over any of Registrar's property; (iv) execution is levied upon any property of Registrar, (v) proceedings are instituted by or against Registrar under any bankruptcy, insolvency, reorganization or other laws relating to the relief of debtors and such proceedings are not dismissed within thirty (30) days of their commencement, or (vi) Registrar files for protection under the United States Bankruptcy Code, 11 U.S.C. Section 101 et seq., or a foreign equivalent or liquidates, dissolves or otherwise discontinues its operations.

5.6 Termination Procedures. This Agreement may be terminated in circumstances described in Subsections 5.5.1 through 5.5.6 above only upon fifteen (15) days written notice to Registrar (in the case of Subsection 5.5.4 occurring after Registrar's failure to cure), with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.8 to determine the appropriateness of termination under this Agreement. This Agreement may be terminated immediately upon notice to Registrar in circumstances described in Subsections 5.5.7 and 5.5.8.

**DRAFT: Potential RA Amendments**

**SPECIFICATION 6**

**REGISTRY INTEROPERABILITY AND CONTINUITY SPECIFICATIONS**

**[…]**

1. **Abuse Mitigation**
   1. **Abuse Contact**. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email address or webform and mailing address as well as a primary contact for handling ~~inquiries~~reports related to malicious conduct in the TLD, including DNS Abuse, and will provide ICANN with prompt notice of any changes to such contact details. Where a webform is used, the webform must not impose unreasonable rate or character limits on submissions, and must allow users to submit attachments up to a reasonable file size limit. Upon receipt of such reports, Registry Operator shall provide the reporter with confirmation that it has received the report.

For the purposes of this Agreement, “DNS Abuse” is defined as ~~malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section) as those terms are defined in Section 2.1 of SAC115 (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>)~~ any activity that makes, or intends to make, use of domain names, the Domain Name System protocol, or any digital identifiers that are similar in form or function to domain names to carry out deceptive, malicious, or illegal activity.

* 1. **DNS Abuse Mitigation**. Where a Registry Operator reasonably determines, based on actionable evidence, that a registered domain name in the TLD is being used or was being used for DNS Abuse, Registry Operator must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse. Such action(s) shall, at a minimum, include: (i) the referral of the domains being used for the DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct action, by the Registry Operator, where the Registry Operator deems appropriate. Action(s) may vary depending on the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage. Where the Registry Operator refers the domains being used for the DNS Abuse under Section 4.2 (i), along with relevant evidence, to the sponsoring registrar, and the sponsoring registrar does not promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping or otherwise disrupting the domain name(s) from being used for DNS Abuse, the Registry Operator shall itself take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping or otherwise disrupting the domain name(s) from being used for DNS Abuse.

~~4.2~~4.3. **Malicious Use of Orphan Glue Records**. Registry Operator shall take action to remove orphan glue records (as defined at https://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct.

**[…]**

**SPECIFICATION 11**

**PUBLIC INTEREST COMMITMENTS**

**[…]**

1. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the Public Interest Commitment Dispute Resolution Process established by ICANN (posted at https://www.icann.org/picdrp), which may be revised in immaterial respects by ICANN from time to time (the “PICDRP”). Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.
   1. 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.

Registry Operator will enforce the provisions of the Registry-Registrar Agreement with respect to these items, including with respect to registrars that experience high rates of DNS Abuse (as a percentage of sponsored domains).

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~~DNS Abuse. Registry Operator will maintain statistical reports on ~~the number of security threats~~ identified DNS Abuse 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.