We welcome the proposed Amendments of gTLD RA and 2013 RAA, and would like to express our respect to the stakeholders associated with ICANN who have compiled the draft. Overall, we highly appreciate the proposed Amendments but find it inadequate in some respects. We are engineers engaged in domain reselling, DNS Content Server and DNS Cache Server operation, hosting service provision, internet access service provision, abuse report reception in Japan. We would like to make our comments from the position of engineers who take responsibilities of those practices, and also in the position of engineers who voluntarily work with the Manga piracy site countermeasure team in Japan (i.e. as a pro-bono activity) at the Working-Level Forum for Anti-Piracy of Japan, where many ICT companies and content holders in Japan gathers.

The Amendments defined DNS Abuse as “malware, botnets, phishing, pharming, and spam”. It is a practical definition and we appreciate it. However, such definition does not fully cover all types of possible DNS and domain name resources abuses by Registered Name Holder. Specifically, the responsibility of registrar has not been stated, when DNS and domain name resources are used for abuses other than forgery websites, for instance, one-click scam websites, lottery scam websites, e-commerce fraud websites, or online piracy sites, illegal trading platforms. We point out that the registrar's liability is not clearly stated in these cases. But at least, we have reason to expect its effectiveness towards URL Hijacking, Cybersquatting, Domain Homograph Attack, Domain Generation Algorithm Malware. Indeed, for abuses not included in the Amendments' definition of DNS abuse, it is often difficult to assess whether the case constitutes abuse without investigating whether the content of the website is appropriate. And since it is not easy to investigate content in the positions of registry or registrar, we appreciate the practicality of the definition. In the meantime, we would like to assert repeatedly, registry or registrar should not be exempted from liability for abuses not included in the Amendments' definition, and such liability can be mitigated if the RAA's Registered Name Holder complies with the conditions related to the accuracy of the information. Specifically, as stated in Article 3.7.7.2 and Article 3.7.8, to verify the information submitted by the Registered Name Holder in accordance with the RDDS ACCURACY PROGRAM.

We agree with clauses of the Amendments draft RAA Article 3.18. Posting abuse contacts conspicuously and readily accessible is important to stop or disrupt abuse promptly. In this case, registrars will probably receive numerous requests from end users, especially consumers that should be directed to hosting providers. Article 3.18.4 is important in this regard.

While Article 3.18 of the Amendments draft is important and worthy of support, we would like to point out that RAA Article 3.18 has no deterrent effect against DNS abuse and as mentioned above, that deterrence is only available if registrars comply with RAA Article 3.7.7.2 and Article 3.7.8, Therefore, it should be noted that Article 3.18 is strongly connected with Article 3.7.7.2 and Article 3.7.8.

We would like to point out the importance of the Registered Name Holder verification program in the "RDDS ACCURACY PROGRAM SPECIFICATION" being implemented by each registrar in accordance with RAA Article 3.7.8. It is critical for freedom of expression and the free flow of digital information on the Internet that the definition of DNS abuse not be excessively bound with the website content. Defining DNS abuse in this way leaves open technical, legal, and social conventional vulnerabilities that could allow the distribution of infringing content or illegal content that could be perceived as fraudulent by the international community. By failing to prevent malicious parties from registering domain names, it facilitates the distribution of illegal content. Therefore, verification of Registered Name Holder information by registrars is extremely important to mitigate this vulnerability.

Verifying the Registered Name Holder's telephone number as indicated in "RDDS ACCURACY PROGRAM SPECIFICATION" 1.f.ii(A) and verifying the address as indicated in 1.f.ii(B) can be effected to some extent. However, it is questionable whether verification of telephone numbers alone is sufficient to stop or disrupt abuse, given that phone numbers are traded on the criminal market and smartphone malwares exist that intercept outgoing and incoming SMS. On the other hand, the address is information that determines which country's investigative body has the authority to investigate, and also information that determines in which country a claim for damages should be filed. It is even more valuable because address information enhances traceability in criminal and civil proceedings, so its verification by registrars should be encouraged. Of course, address verification requires additional verification costs, more time than verifying email addresses or phone numbers, and it is not reasonable to request address verification every time a domain name is registered, transferred, or changes ownership. We are also concerned that overly strict verification of Registered Name Holders may interfere with the right to Internet access, as domain names may be used to create forum for free speech in, for example, countries with low World Press Freedom Indexes. Therefore, we propose a program as an exception to "RDDS ACCURACY PROGRAM SPECIFICATION" Article 3, including "when abuse (not limited to defined DNS abuse) is reported" "additionally verify addresses, etc. when abuse is reported". It should be noted that verification of the email address is not expected to have any effect other than simply "to confirm that the Registered Name Holder can be contacted".

In addition, the Registered Name Holder verification program is important in that it compensates for the deterrent effect on DNS abuse that RAA Article 3.18 lack of. When a registrar terminates a malicious party’s domain, the registrar must share the information verified upon receipt of notification from the Registered Name Holder, for example to share the verified phone number on a block list and prohibit domain name registration by using the same information. If the registrar does not refuse a domain name registration that is related to or matches the verified information about the malicious registrant on the block list, there is no cat-and-mouse game between DNS abuse and takedown. The damage to the abuse will never stop, and the takedown activity will be exhausted.

We expect the RA, RAA to be effectively adhered to by registries and registrars. The total amount of DNS abuse is an urgent problem at the present time in 2023. The background of the problem is the fact that some registrars are not proactive in taking action on DNS abuse, and with the exception of email addresses, there is a lack of verification of Registered Name Holder information by registrars, which may allow a malicious party to register domain with false information, or simply to register a new one when a domain name is suspended as “clientHold”. New registrations can be made over and over again. In addition to this background, some registrars provide big discounts for the first year's domain name registration fee and sets high renewal fees for the following years. Such a business model encourages the registrations of domain names that are intended to be discarded within one year, especially for spamming or other activities that could be placed on the Domain Block List. Domain name registration fees are set by registrars as a business strategy at their own discretion. On the other hand, the domain name registration fee should appropriately include costs for DNS abuse countermeasure and Registered Name Holder verification.

We request that ICANN publish transparency reports that can verify effective compliance of registries and registrars with the RA and RAA. Despite the importance of Domain Abuse Activity Reporting, it is unable to measure the incidents and trends of DNS abuse on a per-registry or per-registrar basis. We request that the DAAR include the number of DNS abuse incidents per-registry and per-registrar in the report.