Suggestions for Improving Current Policies:

1. Both registries and registrars should publish a dedicated email address exclusively for reporting DNS abuse cases, and ICANN should maintain and publicly share an updated list in a machine-readable format (similar to the registrar IANA ID list published on IANA website). At the time of writing, there are 3,020 active registrars listed on the IANA ID page. Currently, reporters must maintain their own email lists and constantly update them as registrars change email addresses from time to time, which is burdensome for frequent reporters. While WHOIS data could be used to extract these email addresses, it requires extra requests and parsing, creating unnecessary overhead. A similar approach should be applied to registries; however, for registries, it would be simpler to have a unified email address (e.g., report-abuse@nic.TLD) to reduce the effort of maintaining an updated list.

2. The email address cannot be replaced by an abuse form. Some registrars require users to submit DNS abuse reports through an online form. While this may be practical for **infrequent reporters** (normal users who report DNS abuse occasionally), it is not practical for **active reporters** who submit reports regularly. These forms are often protected by CAPTCHA or a one-time email code, making automated submissions impossible. While the form can remain as an additional option, providing a dedicated email address should be mandatory.

3. Section 4.2 of the base registry agreement (RA), Approved 21 January 2024, says that:
“registry operator must **promptly** take the appropriate action….” (page 82).
It is important to clearly define what “promptly” means in practice. Does it refer to 24 hours, 48 hours, one week, or another timeframe?
(This is also valid for section 3.18 of RAA).

4. I have observed cases where some registrars “sinkhole” a domain by changing its nameservers to ones under their control. This practice is fundamentally problematic for several reasons:

- **Additional tracking burden:** Reporters must maintain a separate “sinkhole list” to distinguish active from disabled domains, and keep it constantly updated. The easiest approach to check if the domain has been taken down or not is to query DNS records (usually looking for NXDomain response). By sinkholing domain names, the DNS query response shows that the domain name is still alive and this results in re-submitting abuse reports to registries and registrars which waste more time of all parties.
- **Nonstandard method:** Malicious activity can be stopped at the domain level using the EPP status code (e.g., clientHold), which is a standard, measurable way to disable a domain (DNS queries return NXDomain response, and WHOIS data shows the domain status as “clientHold”).
- **Privacy violations:** Sinkholing a domain by mistake exposes legitimate users’ traffic to the registrar or third party without consent. There have been instances where registrars running HTTP servers captured traffic from legitimate domains.
- **Sensitive data risks:** Even sinkholing malicious domains can violate user privacy if URLs contain sensitive information, such as victims’ credentials.

Some may argue that sinkholing is a common practice in cases of malware and botnets (for example, Shadowserver did this for Avalanche operation). However, it is important to note that in malware and botnet cases, sinkholing is used to alert ISPs about the infected machines so they can notify the victiom about his infected machine. In contrast, why do registrars sinkhole domains for phishing attacks? Is it to notify victims, facilitate cleanup procedure or collecting data?

5. At some point, the DNS ecosystem will need a solution similar to the certificate transparency log—often referred to as a **DNS transparency log**, as suggested by SSAC125 and the Internet Fire Brigade. Such a log would allow security experts and organizations to instantly access changes in zone files, enabling real-time monitoring of newly registered domains. This, in turn, would make it possible to detect malicious activities more quickly and effectively. By significantly reducing the uptime of maliciously registered domains, a DNS transparency log could potentially be as effective as proactive mitigation measures. Currently, the CZDS allows the community to download zone files only once every 24 hours. This update interval provides attackers with enough time to carry out malicious activities. In many cases, a newly registered domain can be observed in the certificate transparency log, but only if the attacker issues a TLS certificate for the domain. Furthermore, by issuing a wildcard certificate, attackers can often conceal malicious subdomains, making detection even more difficult.

In my opinion, implementing these five points could significantly improve current DNS abuse mitigation procedures and appears more practical than the two proposed solutions.