The gTLD Registries Stakeholder Group (RySG) appreciates the opportunity to comment on Question 4 and Question 5 of ICANN’s Preliminary Draft Framework for Registry Operators to Conduct Periodic Security Checks and Respond to Identified Security Threats (“Preliminary Draft Framework”). We wish to reiterate some general comments from the comments previously submitted by the RySG on the Preliminary Draft Framework, which apply equally to Question 4 and Question 5, as well as to provide specific comments related in response to these questions.

**General Comments**

**Clarifications or best practices documents published by ICANN ex post facto must not be treated as new registry requirements or as standards for ICANN Compliance.**

As noted in our January 29 comments, the Registries Stakeholder Group (“RySG”) is concerned that a “best practices” document published by ICANN would be misconstrued as creating new requirements for all Registry Operators. It was generally agreed in a meeting between Registry Operators and ICANN staff during the ICANN 52 Public Meeting in Singapore that additional guidance should be framed as an example of one monitoring approach that would satisfy the requirements for Specification 11, Section 3(b) and not as a universal minimum requirement, a “best practice,” or a standard deployed by ICANN Compliance in evaluating audit or compliance inquiry responses. ICANN’s final proposed framework cannot constitute binding contractual requirements unless and until it successfully passed through the Policy Development Process. The RySG would object strongly to it being treated as otherwise by ICANN’s compliance team.

Moreover, ICANN should separate the notion of a “framework” intended to respond to security threats from guidance on contractual compliance. As we discuss below, issues of response to security threats fall outside the scope of Specification 11, Section 3(b), therefore a framework including a response element is necessarily not related to issues of contractual compliance or interpretation. Separating compliance guidance from the development of a framework for identifying and responding to security threats will allow for an appropriate focus on communication and coordination in responding to these threats rather than conflating the discussion with the narrow requirements of Specification 11.

**Constrain the scope of discussion to “security threats” and establish an agreed upon working definition of “security threats.”**

The discussion language provided by ICANN pursuant to Framework Questions 4 and 5 repeatedly makes reference to “malicious conduct/behavior and criminal activities,” categories which far exceed the “security threats” referenced in Specification 11, Section 3(b). Further, monitoring for and enforcement of broader criminal activity could not reasonably be addressed through the monitoring processes contemplated in Specification 11, Section 3(b) and enforcement would require registries to make judgments typically handled by law enforcement agencies.

We believe that this intended “clarification” of the “security threats” actually adds additional ambiguity, and that it should no longer be used in the development of a potential framework.

**Feedback provided herein and on the Working Group list are initial responses only and must not be interpreted as Registry approval of the Preliminary Draft Framework.**

As previously noted, this internal discussion and feedback exchange is not and must not be taken to constitute RySG approval of or acquiescence to ICANN’s final proposed Framework. The Preliminary Draft Framework is very high-level in nature. It does not paint a sufficiently clear picture of the new requirements that ICANN seeks to impose on Registry Operators to permit the e RySG to provide more substantive comment.
Preliminary feedback by a small number of registries must not be construed as RySG support for the final output by ICANN, or for any aspects of the Preliminary Draft Framework.

Further, we note that the RySG has yet to receive a response from ICANN on the comments previously submitted on January 29, nor the additional feedback provided during the topical meeting during the ICANN 52 Public Meeting in Singapore. ICANN must provide the RySG with additional opportunities to comment after the Preliminary Draft Framework reflects this feedback.

**Framework Question 4: What actions (e.g., mitigations) should be taken in response to such identified security threats?**

Mapping particular actions or mitigations to identified security threats is outside of the scope of Specification 11, 3(b).

Specification 11, Section 3(b) requires that registries provide statistical reports about the actions taken in response to identified security threats; it does not require registries to undertake a particular course of action in response to an identified threat. In previous conversations with the Registries Stakeholder Group, representatives of ICANN staff have asserted that the goal of the Preliminary Draft Framework was to provide guidance for how the requirements of the Specification 11, Section 3(b) could be met. Mapping particular actions to identified security threats is not required by and is beyond the scope of Specification 11, Section 3(b) and, as such, would not further the stated goals of the Preliminary Draft Framework.

Any effort to include responses to identified security threats in the proposed final Framework must be understood to be outside of Specification 11 and registry operators’ contractual responsibilities. Such a framework should instead focus on providing mechanisms for communication and identifying the set of problems where DNS intermediaries can provide an appropriate part of the response. The framework should focus on information sharing and reporting (previously discussed in our response to Question 3) rather than on direct mitigation.

**Registry Operators may already have established policies for handling certain threats that are incorporated into existing Registry-Registrar Agreements and/or Registration Agreements.**

In addition, introducing new Registry Agreement requirements now is problematic from a contractual standpoint. Many registries have already developed acceptable use policies and abuse procedures for their TLDs. These policies are, in many cases, incorporated into executed contracts, such as Registry-Registrar, which may also include required language and terms for Registration Agreements. Introducing new, standardized acceptable use policies and abuse procedures could require registries to take actions not currently provided for in these arrangements and require registries to violate their contracts with registrars or the registration and acceptable use policies agreed to by their registrants.

**Action by a registry is often not the most effective means of mitigating identified security threats.**

As noted in discussions during the ICANN 52 Public Meeting in Singapore, the registry is often not the most effective nexus for mitigating abusive activity in the DNS. Hosting and network providers are often better positioned to remedy abusive activity and to aid in investigations of identified security threats. Similarly, as domain names are necessarily sold through registrars, registries do not maintain a direct contractual relationship with registrants and may be limited in their ability to contact registrants directly.

As such, registries have extremely limited ability to take intermediate measures to mitigate identified security threats, short of suspending or deleting the domain name in question. For many identified threats, the registrant may be unaware of and not directly involved in the abusive activity in question, making domain name suspension or deletion an action of last resort.
Further work on the Preliminary Draft Framework should include an assessment of what, if any, of the threats identified in Specification 11, Section 3(b) are most appropriately handled by the registry, and which are better handled by other actors who have direct contact with the registrant and/or content provider(s), such as hosting providers or registrars.

**Investigation of threats is required to determine appropriate action; neither pattern detection nor the reputation of the information source are sufficient to warrant action without review.**

Human review and assessment of threats remains an essential prerequisite to taking action on any domain name. The input provided by ICANN security staff recommends the use of automatic pattern detection and programs such as the APWG’s Accelerated Malicious Domain Suspension program as guides for how registries should respond to identified security threats to reduce the uptime of affected domains and expedite the suspension process, respectively. While these resources may provide useful tools for security monitoring under Specification 11, Section 3(b), they are not infallible. Without the additional step of human review and assessment of a particular threat, these sources cannot justify actions such as suspension of a domain name.

“False positives” resulting in domain name suspension without adequate human review and assessment expose a registry to significant liability risks. Given the millions of domain names in the DNS, even “extremely low” rates of false positives could result in the unwarranted suspension of many domain names and introduce liability risks for Registry Operators. If ICANN imposed upon Registry Operators a requirement to respond to identified security threats in a particular manner, we would expect that ICANN indemnify Registry Operators in the event that one or more false positives resulted in litigation against the registry. This is not currently supported within the New gTLD Registry Agreement.

**Framework Question 5: What are the relevant metrics for reporting on actions taken in response to malicious conduct or criminal activities?**

Providing quantitative statistics of the actions taken in response to identified security threats is generally appropriate and within the contemplated scope of Specification 11, Section 3(b), provided that such actions are determined by the Registry Operator upon appropriate review and investigation, and not mandated in a top-down fashion for the reasons outlined above.

**Self-reported comparative statistics may not accurately demonstrate the efficacy of security monitoring offerings and may introduce additional concerns.**

However, we have several concerns related to the introduction of “efficacy statistics,” or measures for comparable periods to show changes to the number of threats reported over time. First, requiring these metrics introduces new data points that may not have been accounted for in designing security monitoring services.

The provision of comparative statistics over time also assumes that reports are generated on regular intervals that are appropriate for comparing threat occurrence. Monitoring services may, in fact, generate information on shorter intervals that render these metrics less meaningful, or on flexible intervals that are not easily compared.

Further, describing these metrics as “efficacy statistics” falsely suggests that these statistics effectively measure the performance of security monitoring services. While effective monitoring and mitigation may affect such metrics, other environmental factors could affect these metrics such as overall activity rates for the threats under consideration, changes to registry policies, changes to activities carried out by other parties (e.g. registrars, hosting, or network providers), the fraction of incidents in which the registry was the proper nexus for taking action against the identified threat.
We also have serious concerns about the possibility of gaming if self-generated and reported “efficacy statistics” are used to rank order TLDs and service offerings. Services offerings will inevitably vary in the types of threats that they identify. Comparing the rates of change in threat occurrence across TLDs would not account for this diversity, and could incentivize registries to conduct less-thorough monitoring or to under-report identified threats, rather than to improve their service offerings. Lastly, we have grave concerns that network providers may use the publication of such metrics as justification for blocking access to certain TLDs regardless of how robust the registry operator’s detection and mitigation strategies may be.