We appreciate the opportunity to comment on ICANN’s Preliminary Draft Framework for Registry Operators to Conduct Periodic Security Checks and Respond to Identified Security Threats (“Preliminary Draft Framework”). We provide, first, some general comments related to the proposal to introduce requirements for Registry Operators conducting technical analyses of security treats in their TLD(s) pursuant to Specification 11, Section 3(b) (“Technical Analyses”) and the process by which it has been brought forward, as well as responses to the questions posed by ICANN for registry feedback by January 30, 2015.

General Comments

It is not clear that the objectives of the intended framework can be best fulfilled via gTLD registries. In fact, the specific questions being posed by in ICANN’s Draft Framework are likely premature without some initial discussion about the appropriate roles of ICANN, registries, registrars, registrants and other parties. As a preliminary matter, we suggest that this process be “rebooted” with an opportunity for discussion of both high level goals as well as a community-driven process to arrive at an appropriate framework for both identifying and responding to security threats.

We note the following high-level concerns and questions relating to the proposed framework:

1. Industry is already dealing with the issue of security threats to the domain name system outside of ICANN.
2. Through the Preliminary Draft Framework, ICANN is striving to become a Clearinghouse for threat indicators. The appropriate role of ICANN and other actors in both the domain name and security community needs to be better defined before developing this type of framework.
3. Through the Preliminary Draft Framework, Registry Operators are being asked to incur risks including possible liability but are not indemnified in any manner.
4. The Preliminary Draft Framework does not include metrics for how collateral damage will be evaluated and addressed.
5. By taking a prescriptive approach to identifying security threats, ICANN may quash innovation and the opportunity to quickly develop responses to emerging types of threats, and it may be possible for one registry or registry partner to game the Preliminary Draft Framework to create a captive market for the provision of services related to Specification 11 3(b).
6. The Preliminary Draft Framework does not improve clarity in the definition of the types of risks being addressed.
7. Registries are not qualified to determine “criminal behavior”.
8. The Preliminary Draft Framework alludes to current best practices but they are not defined.
9. The Preliminary Draft Framework does not address whether and how implementation will vary across jurisdictions.

A few of these are discussed further below.

What are the ‘industry experience’ and ‘best practices’ often referenced in the framework?

The best practices or industry experience should be specifically referenced instead being generally named. It is unclear whether the best practices referred to appear in a BCP, RFC, or SSAC advisory; if so, the advisories should be specifically named.
Efforts to standardize security reporting and response practices are untimely and would introduce new and unanticipated costs for Registry Operations

The Specification 11 requirements were immediately effective for all registries from their date of launch, which for the earliest new gTLDs began in early 2014. As such, registries have been left to define and apply their own standards for these Technical Analyses. Publication of a standardized framework for these requirements would inevitably align with certain offerings over others; this could include services that are protected by patent creating an effective monopoly in the market. Even presented as a “best practices” document, efforts to standardize Technical Analyses would create winners and losers in a preexisting market. Registry Operators have invested money and effort in developing services to meet the requirements of Specification 11, Section 3(b), or have entered into subcontracting arrangements to meet these requirements. Redefining scope and nature of required Technical Analyses at this juncture may result in registries or their service providers needing to reengineer their services or enter into new arrangements to meet requirements that were not specified at the time of contracting. These burdens would likely apply even to services that met all contractual requirements and were effectively deterring and addressing security threats in new gTLDs.

Clarifications or best practices documents published by ICANN ex post facto must not create false expectation regarding registry requirements, nor be treated as standards for ICANN Compliance

Given ICANN’s singular role in monitoring registry and registrar compliance, we are concerned that, if it were published by ICANN, even a “best practices” document, it would be misconstrued as new requirements for all registries.

We note that in discussions around the Preliminary Draft Framework ICANN has been reluctant to affirm whether a final Framework would be used by ICANN’s compliance team in issuing compliance requests or evaluating the sufficiency of responses to such requests. This ambiguous description in the Preliminary Draft Framework of the interplay between the implementation of the “minimum requirements” of the Preliminary Draft Framework by Registry Operators and compliance with Specification 11, Section 3(b) exacerbates, rather than resolves, this uncertainty. The Preliminary Draft Framework indicates that “it is anticipated” that compliance with the minimum requirements of the Framework would be voluntary, and that failure to implement the standards “would not necessarily mean” a contractual violation is taking place. Unless it successfully passed through the Policy Development Process or the amendment procedures delineated in Registry Agreement Articles 7.6 or 7.7, the final framework cannot constitute binding requirements and we would object strongly to it being treated as such by ICANN’s compliance team.

We urge ICANN to align its compliance practices and its description of those practices in the Preliminary Draft Framework with what is provided for in its contracts with Registry Operators.

Establishing consistency and clarity in the definition of “security threats” is an essential first step in obtaining meaningful comment from the community on the Preliminary Draft Framework.
Specification 11, Section 3(b) requires Registry Operators to assess whether domains in the TLD are being used to perpetrate “security threats, such as pharming, phishing, malware, and botnets.” The NGPC Proposal, in turn, directed ICANN to solicit community participation “to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences.” Without further explanation, the Preliminary Draft Framework has replaced “security threats” with “malicious conduct or criminal activity” “in the interest of clarity” throughout the Draft Framework’s questions and discussion. Rather than add clarity to the discussion, ICANN has both made the discussion less clear by replacing “security threats” with two terms that are even less well defined and potentially expand the scope of Specification 11 (b) into areas completely unrelated to security threats. In addition, the Draft Framework raises significant concerns and questions over what constitutes “malicious conduct or criminal activity” and what laws, principles, jurisdiction, and authorities are relevant. Without properly defined terms from which to begin, meaningful comment on the substantive questions regarding the Preliminary Draft Framework is impossible, and formalizing the definition of “security threats” is an essential first step in ensuring that the Framework does not exceed or expand upon the requirements contained in Specification 11.

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

We appreciate ICANN’s efforts to engage Registry Operators in the development of the Preliminary Draft Framework. However, this internal discussion and exchange of feedback must not be taken to constitute registry approval of or acquiescence to the final Framework produced by ICANN. 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 this community to comment. Preliminary feedback by a small number of registries must not be construed as Registry support for the final output by ICANN, or for any aspects of the Preliminary Draft Framework. Overall, we view this exercise as premature given that the appropriate roles and responsibilities of the various parties have still not been discussed nor agreed upon.

Comments on Framework Question #1:

What is the nature and scope of an appropriate set of technical analyses to assess which, if any, domains in a TLD are being used to perpetrate malicious conduct or criminal acts), such as pharming, phishing, malware, and botnets?

Defining a standard nature and scope for the Technical Analyses is problematic for several reasons. First, the considerations around nature and scope discussed in Framework Question 1 exceed what is contemplated in Specification 11. Expanding and standardizing the scope and of the required Technical Analyses at this juncture could introduce additional costs and burdens that were not contemplated at the time of contract execution, even in instances where current practices were fit for purpose. Second, new gTLD registries are highly diverse and the types of “security threats” referenced in the Preliminary Draft Framework often do not occur within the DNS. Variables including size, registration policies, registration/verification procedures, and cost, among others, have significant impacts on the relative
risk profiles of new gTLDs. These risk profiles have implications for the activities that should be carried out in a Technical Analysis.

The discussion under Question #1 goes on to say: “If endorsed by the ICANN community, ICANN could provide Registry Operators with a recommended (preferred and trusted) set of such “block” lists, and could allow registries to identify other lists that would be added to the trusted set upon ICANN’s approval.” This proposition raises several concerns. First, the identification of preferred and trusted block lists and services seems to be outside of ICANN’s limited technical coordination mission for Internet identifiers and area of expertise. The market for reputation service providers and other security resources is established and growing; many service providers and offerings are widely recognized and highly effective, regardless of whether they are endorsed by ICANN. As is currently permitted, registries must be able to define and rely upon their own “trusted list” of reputation service providers and other resources in conducting their Technical Analyses. In addition, registry operators may have internal resources that enable the type of analysis and detection contemplated by Specification 11. The “trusted list” of reputation service providers referenced in the Preliminary Draft Framework provides useful examples of reputation services that may be consulted in this process, provided that they were made available to registries and their partners at a reasonable cost. However, these reputation services are, in many instances, overlapping. Consultation with each of the sources referenced must not be a requirement. Use of each of these services places costs on the Registry Operator, particularly in investigation and validation efforts, as no reputation service offers completely accurate and timely security threat information. Unfortunately these investigation and validation costs may not be fully removed by the use of automated techniques for analysis of domains as these techniques continue to suffer from false positives. Based upon the size and nature of the registry and the other procedures being carried out in the Technical Analysis use one or more of the sources referenced, may also not be necessary to yield highly accurate reports and effective handling of security threats. Similarly, registries must not be required to seek approval from ICANN to add additional services or resources to their individual “trusted list.” The list in the Preliminary Draft Framework is non-exhaustive and the field of security services is constantly evolving. This requirement could undermine the further development and refinement of registries’ Technical Analyses.

We also note that one of the most useful sources of threat intelligence to registries, its own abuse-handling department (or contact), is not listed in the current version of the framework. While such channel is probably useful for all registries, and mandated by registry agreements, for some registries (depending on the previously mentioned variables) this could suffice as the single source of information.

Further, a domain name by itself is rarely the direct vector for security threats, and attempts to conflate content or services referenced by domain names with the DNS itself could be a very slippery slope.

Note the following statement in the last paragraph under Question #1: “In assessing whether a reported domain name is actionable, consideration should be given to appropriate means of verifying that the alleged use of the domain is genuinely malicious or criminal and not resulting from errors in the reporting process or by the reporting entity.” As elaborated upon below, the qualifiers “malicious or “criminal activity” appear to go well beyond the intended scope of the Preliminary Draft Framework: to
provide guidance for responding to security threats. The expectation that registry operators be fully capable of evaluating malicious and criminal activity would introduce significant new roles and responsibilities for Registry Operators and potentially conflate roles that are typically associated with law enforcement agencies. Qualifying all domain names that are malicious or criminal would be incredibly burdensome for registry operators. Registry operators are not in themselves capable of or empowered to evaluate all malicious or criminal content, particularly when the cross-border nature of the internet is taken into account.

Comments on Framework Question #2: How frequently should Registries conduct such technical analyses?

Due to the diversity of new gTLD risk profiles the appropriate frequency of Technical Analyses will vary widely from new gTLD to new gTLD. We agree, generally, that data collection should be a relatively regular activity; however, even this basic requirement may be inappropriate for a new gTLD focused around a small set of SLDs. The references to automated and non-automated analysis of the data are not contemplated within Specification 11, Section 3(b) and should not have an associated frequency.

Note the input from ICANN security staff on Question #2: “Best practices would suggest collection of data and automatic recognition of anomalies, patterns or other specific criteria should be performed with relatively high frequency, e.g., daily, weekly or monthly. Similarly, processing and analysis of the data and generation of reports should be performed with sufficient frequency, e.g., quarterly, to allow detection of significant changes but not so frequently that reporting captures little or no data (as would be the case for TLDs with infrequent changes).” What ‘best practices’ are referred to here? What are the policy and legal implications of data collection and privacy?

Comments on Framework Question #3: What should be the relevant metrics for reporting on malicious conduct or criminal activities as a result of such technical analyses?

Specification 11, 3(b) states the required metrics for reporting with respect to the Technical Analyses: the number of security threats identified and the actions taken as a result of periodic security checks. Additional metrics, beyond those provided for in the Registry Agreement, must not be required in ICANN compliance inquiries.

As is the case throughout the document, Question #3 needs to be revised to change “malicious conduct or criminal activities” to “security threats.”

Great caution must be taken in trying to cross-compare and draw conclusions from self-reported metrics; practices and standards for monitoring and reporting will inevitably differ widely across registries and service providers. As a result, this reporting must not be used to identify “good” and “bad” actors in the new gTLD registry space nor to target compliance activities to specific registries or registrars, as it may tend to have a chilling effect on accurate reporting.
Conclusion

The RySG believes that the Draft Framework does not adequately lay the groundwork to determine the appropriate role for gTLD registry operators, ICANN or other parties in developing a framework for detecting and responding to security threats. ICANN seems to be drastically underestimating the amount of resources required for the expanded scope of its “Internet Scale Policing” by registries and it is not clear that ICANN has the required operational core competencies “clearing house for threat indicators”, assuming that the community agreed that this was an appropriate expansion of its mission. There is a gap between the overall simplistic nature of the Preliminary Draft Framework and just how complex this mission space is. The framework underestimates what capability would be needed in the way of legal, policy, law enforcement, commercial and nation state liaisons, cyber technical and non-technical intelligence collections (in a variety of different languages), data automation and analytics at scale, operational process and procedures, analytical tradecraft, and the diverse set of cyber security disciplines to implement the Preliminary Draft Framework as currently proposed. ICANN needs to fully take into account these factors and develop a framework that is appropriate given the roles, responsibilities, and capabilities of Registry Operators, as well as the nature of the Domain Name System. We believe considerably more discussion is required to establish basic principles related to the framework before in-depth discussion of registry detection or reporting processes is appropriate.

RySG Level of Support

1. Level of Support – Active Members: N/A
2. Minority Position(s): None
3. List of voting and non-voting members:
   1. Afilias, Ltd.
   2. Charleston Road Registry (non-voting member)
   3. .CLUB Domains LLC
   4. China Organization Name Administration Center (CONAC)
   5. CORE (non-voting member)
   6. DNS Belgium vzw
   7. Donuts Inc.
   8. DotAsia Organisation
   9. dotBERLIN GmbH & Co. KG
   10. dotCooperation (inactive)
   11. Dot Kiwi Ltd.
   12. Dot Latin, LLC
   13. DotShabaka Registry
   14. dotStrategy Co.

1 No formal votes were taken on the foregoing comment. While the RySG engaged in substantive debate about particular issues related to the comment and Preliminary Draft Framework more generally, the comment reflects the outcome of such discussions and has broad stakeholder group support. No members raised objections to the submission of the comment.
15. Employ Media LLC
16. European Broadcasting Union (EBU)
17. Famous Four Media
18. Foundation for Assistance for Internet Technologies and Infrastructure Development (FAITID) (non-voting member)
19. FTLD Registries LLC
20. Fundació puntCAT (inactive)
21. GMO Registry, Inc. (non-voting member)
22. ICM Registry LLC
23. InterNetX Corp. (non-voting member)
24. IRI Domain Management, LLC
25. KNET (non-voting member)
26. Minds + Machines
27. Museum Domain Management Association – MuseDoma (inactive)
28. National Association of Boards of Pharmacy (NABP)
29. National Association of Real Estate Investment Trusts Inc.
30. Neustar, Inc
31. Nomiinet
32. Nucleo de Informacao e Coordenacao do Ponto BR (NIC.br)
33. OP3FT
34. Plan Bee LLC
35. Public Interest Registry - PIR
36. Punkt.wien GmbH
37. Punkt Tirol GmbH
38. Punto 2012 S.A. de C.V.
39. Radix FZC
40. Region D Alsace
41. Richemont DNS
42. Rightside Registry (non-voting member)
43. Societe Internationale de Telecommunication Aeronautiques – SITA
44. Sky IP International Ltd.
45. Starting Dot Limited
46. Telnic Limited
47. The Foundation for Network Initiatives “The Smart Internet”
48. Top Level Design LLC
49. Tralliance Registry Management Company (TRMC)
50. Uniregistry Corp. (non-voting member)
51. Universal Postal Union (UPU)
52. VeriSign
53. XYZ.COM LLC
54. Zodiac

- Names & email addresses for points of contact
  - Chair: Keith Drazek, kdrazek@verisign.com
  - Alternate Chair: Paul Diaz, pdiaz@pir.org
  - Secretariat: Cherie Stubbs, rysgsecretariat@gmail.com
  - RySG representative for this statement: Stephanie Duchesneau, stephanie.duchesneau@neustar.us