Cybersecurity Tech Accord Response*: Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2*

January 22, 2021

The Cybersecurity Tech Accord is grateful for this opportunity to provide feedback and input regarding the recommendations produced by ICANN's Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data (EPDP). Since 2018, our signatories, representing technology firms from across the globe, have noted with concern the dangers posed by what is now a years-long interruption in the regular access to registration data that has historically been a cornerstone in promoting security and accountability online. In addition to our input on Priority 2 recommendations #19-22, please also see below for our more general comments on the process itself, especially in the context of the evolving policy environment.

While we regret that finding meaningful solutions has remained elusive, we nevertheless appreciate this opportunity to provide input and stand ready to answer any questions and provide further support and guidance as necessary. Please do not hesitate to reach out to our Secretariat: info@cybertechaccord.org

Reiteration of Previously Expressed Overarching Concerns

The Cybersecurity Tech Accord wishes to reiterate and support the concerns detailed in the minority statements from the BC, IPC, ALAC, GAC and SSAC, as well as the concerns of NTIA, (delivered to United States Senator Wicker on Dec 23, 2020*)* that argue the policy in the Phase 2 Final Report fails to meet the needs of users of WHOIS data. We strongly urge the Board to carefully consider these concerns in their future deliberations and ensure that any future SSAD*,* and any related consensus policy**,** is indeed fit for purpose and in fact meets the needs of its users.

We also want to remind the ICANN Board of the Letter sent to the EC on the need to restore urgently needed access to WHOIS data. This letter, signed by the Cybersecurity Tech Accord and 20 other organizations, outlines and supports our views that the ICANN Phase 2 policy is not fit for this purpose and is dangerously out of balance, and thus further action from EU Governments will be needed to not only clarify but rectify this situation. [A copy of this letter has been attached to the accompanying email of this submission, for reference]

Considerations regarding the surrounding policy environment

The EPDP deliberations and recommendations have not been happening in a vacuum and are likely to be impacted by recent policy developments. Therefore, we feel EPDP proposed policies and related implementations (based on assumptions of how GDPR should be applied to WHOIS), should be halted for the time being as a result of the following:

1) The European Commission's newly adopted proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) that directly implicates how WHOIS should operate under the GDPR; and,

2) The United States' funding bill, signed into law in Dec 2020, which directly impacts EPDP proposals regarding WHOIS:

> *From the legislation: NTIA [National Telecommunications and Information Administration] is directed, through its position within the Governmental Advisory Committee to work with ICANN to expedite the establishment of a global access model that provides law enforcement, intellectual property rights holders, and third parties with timely access to accurate domain name registration information for legitimate purposes. NTIA is encouraged, as appropriate, to require registrars and registries based in the United States to collect and make public accurate domain name registration information.*

Moving forward with EPDP recommendations in light of these two directly relevant and likely impactful policy changes would seem reckless and a waste of community time. They require ICANN's close attention and the re-evaluation of previous recommendations before moving forward. While certainly much work has already been done, failing to address and respond to the implications of these developments by ignoring them is not in the public interest.

Specifically, the Phase 1 and Phase 2 policies should be reviewed, recommendation by recommendation, to determine how they might be impacted by these developments. For example:

- Recs #1-18 in the Phase 2 report (related to the SSAD) should not be approved
- Rec #4 in the Phase 1 report (fails to improve the accuracy requirements applicable to WHOIS) need to be revisited
- Rec#7 in the Phase 1 report (impacts Thick WHOIS) should be suspended
- Rec #12 in the Phase 1 report (does not require the contact data of legal persons to be published) should be suspended
- Rec #18 in the Phase 1 report (standardizes the request templates) should be implemented in part, with updated timelines and disclosure requirements that track the NIS2 proposals

These are just a few examples. Until such a review of Phase 1 & 2 is conducted, the Temporary Specification should be continued to be enforced. Nevertheless, please see below for the Cybersecurity Tech Accord's specific comments on Priority 2 recommendations #19-22.

Comments on Recommendations #19-22

Recommendation #19. Display of information of affiliated and/or accredited privacy/proxy providers

The Cybersecurity Tech Accord generally agrees with Recommendation #19 as set forth in the EPDP Phase 2 report and would like to make two (2) additional points with respect to this recommendation:

1) While we appreciate that the EPDP Working Group has recognized problems with the redaction of domain name registration data by privacy/proxy services, we are concerned that Recommendation #19 does not go far enough when a request is made for the underlying data behind a privacy/proxy registration. According to the 2013 RAA Section 3.7.7.3:

Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it discloses the current contact information provided by the licensee and the identity of the licensee within seven (7) days to a party providing the Registered Name Holder reasonable evidence of actionable harm.

As set forth above, under 3.7.7.3 of the 2013 RAA, a registrar is required to disclose the underlying contact information or face potential liability for the wrongful use of a domain name. At least one Cybersecurity Tech Accord signatory has found that upon a legitimate request for underlying data, a privacy/proxy service will sometimes remove the privacy/proxy service information, update the registration record to "redacted," and then require a subpoena or other legal mechanism in order to reveal underlying registrant data. In some cases, even if the underlying contact information is inaccurate, the registrar will remove the privacy/proxy service and simply publish the inaccurate data. The data requestor is then required to start again and, in certain cases, file an inaccurate data report. This delays the obtaining of valuable data necessary to uncover nefarious actors using domain names for wrongful purposes in a timely fashion. To that end, there should be a mandate that a registrar collect, maintain and disclose accurate information upon legitimate requests for redacted registrant data of a privacy/provider service.

2) We believe that a domain name record should prominently flag the fact that a domain name registration is with a privacy/proxy service. Currently, it is difficult to determine if a domain name registration is in fact a privacy/proxy registration. There is no standard language used by domain name registrars to indicate that a record is in fact a privacy/proxy registration. In the Privacy Proxy Service Accreditation Issues (PPSAI) report, it was recommended that a field in the domain name record be added which clearly indicates that a domain name is a privacy/proxy registration. The need for this clarification has existed for years. We therefore urge the GNSO to further clarify and implement the recommendation set forth in the PPSAI.

Recommendation #20. City Field

The Cybersecurity Tech Accord notes that the EPDP has improved the policy by removing the "MUST" language regarding redaction of the City data field, which is often necessary for cybersecurity investigations, and for establishing jurisdiction or even identifying the controlling law in a potential lawsuit against a registrant. However, the change from "MUST" to "MAY" is unfortunately unlikely to have any significant practical effect given that (i) the status quo for contracted parties is currently to redact the field, and (ii) many contracted parties resisted even the permissive change to "MAY." Given the *de minimis* likelihood of infringement on registrants' privacy rights versus the benefits to cybersecurity interests, on balance we advocate a policy that requires publication of the City field.

Recommendation #21. Data Retention

The Cybersecurity Tech Accord supports the establishment of a data retention period, as is often required by data protection laws. The EPDP establishes a retention period based on the Transfer Dispute Resolution Policy (TDRP) which, in and of itself, is not problematic. However, we feel this recommendation too narrowly describes the standard for third-party requests during this retention period as "purposes other than TDRP" (the purpose for which data would currently be processed by the registrar). The correct standard is the broader "purposes other than those for which the data was collected," which includes TDRP, among others (GDPR Art. 5.1(b)).

While we understand that ICANN and the contracted parties are currently developing a data processing agreement in order to define roles and responsibilities, the characterization of ICANN Compliance as a potential "Requestor" here is incorrect since ICANN is a controller by data protection principles. As noted in Recommendation #22 (below), at least one of the purposes for the collection of the data belongs to ICANN. The Cybersecurity Tech Accord would also like to note a potential issue caused by the use of the passive voice with "deemed necessary." It will be important for ICANN, when it attempts to enforce this language, to hold responsibility for deeming which data elements are necessary. If contracted parties have the authority to deem which data elements are necessary, ICANN will be unable to enforce this provision.

Recommendation #22. Purpose 2

We support the updated "Purpose 2" as defined in the EPDP Phase 2 Final Report and agree that it should be added to the EPDP Team Phase 1 purposes, which form the basis of the new ICANN policy. However, while it is important to define a purpose for ICANN, it is equally important that 3rd party purposes also form the basis of the new ICANN policy, as stated in NIS 2 Directive, since the NIS 2 Directive explicitly declares that the 3rd party purposes represent a defined legitimate interest.

As the status of the policy agreed to in the Phase 2 EPDP Final Report is far from clear and the timing of any approval and implementation is many years away, the third party purposes defined in Recommendation #7 in the EPDP Phase 2 Final Report must also be added to the EPDP Team Phase 1 purposes, which form the basis of the new ICANN policy. Not doing this would result in an incomplete, underspecified and ultimately ineffective policy.

Sincerely,

The Cybersecurity Tech Accord

Cybersecurity Tech Accord (cybertechaccord.org)