15 April 2019

TO: Technical Study Group (TSG)

gdrp@icann.org,

FROM: iThreat Cyber Group

RE: comments on the "Draft Technical Model for Access to Non-Public Registration Data", draft of 6 March 2019

The volunteers of the TSG have performed a great deal of work in a short time, and present some excellent ideas that further the conversation considerably. Below we offer a constructive examination. There are three areas where the work has weaknesses:

A. The TSG recommended Model 3, which is more complex and burdensome than a viable alternative, Model 2. It's unclear why.
B. The paper does not adequately take into account the needs of the requestors. The requestors are the main users of the system, for whom RDS services are designed and for whose benefit they are maintained. As a result, some important technical requirements have not been taken into account or balanced.
C. The TSG has exceeded its remit and made policy recommendations.

The project contains some excellent work. The forthcoming final draft can serve as a map for further review in the community, and can receive improvements and evolve over time. But for the reasons above, it cannot be positioned as an implementation specification, or a *fiat accompli.*

ACTOR MODELS

The TSG appears to recommend Model 3, which is more complex, more burdensome, and may provide poorer performance than Model 2. The draft does not adequately explain and justify the choice. Notably, Model 3 relieves ICANN Org of some work that it can and perhaps should be responsible for. The TSG must more clearly lay out the consequences and drawbacks of these models, documenting the reasons for its recommendation.

Model 1 is clearly not viable because it would have ICANN decide what parties should be authorized requestors. The way to solve that problem is by involving Identity Providers. The core role of an Identity Provider is to vet potential authorized requestors and recommend them to ICANN for approved access.

But then there are two ways to involve the Identity Provider:

a) The Identity Provider can tell ICANN's who's authorized to make requests, and then ICANN would handle management of the technical credentials that requestors use to access ICANN's gateway. *This is the TSG's Model 2*. Or,
b) The Identity Provider must both vet users AND handle the requestors' credentials to the ICANN gateway including issuing and maintaining the technical credentials. This requires the Identity Provider to have a core operational and technical role with the system. T*his is the TSG's Model 3.*

Model 2 is simpler than Model 3. In Model 2, a query requires four hops, with three parties involved[1]. Model 3 may require six hops and four operational parties.[2] This model may therefore perform more slowly for all users. And it adds another point of failure.

But the TSG appears to recommend Model 3 – although oddly the TSG does not say so explicitly. The paper's "Proposed Solution" section seems to describe a Model 3 solution in which the Identity Provider will issue tokens for RDAP queries, states that the Identity Provider will be measured for SLAs while doing so, etc. The "Proposed Solution" also adds in mandatory Third Party Authorizers, yet another function that adds complexity

Having Identity Providers in a highly operational role, and involved to such a degree in the system's functioning, may not be necessary. And it does not fit with the TSG's principle that "burdensome complexity should be pushed, when possible, to the fewest and most capable actors" and that "The largest contingent of actors in this system will be the requestors, for example law enforcement agents. Any proposed solution should attempt to keep burdensome, complex and technical matters from impacting their primary duties." For example the TSG's "Proposed Solution" seems to push complex technical execution directly onto law enforcement, which will need its own Identity Provider(s). *The extent of the Identity Provider's role is a policy decision, not a purely technical one for the TSG to decide.*

And depending on implementation, *Identity Providers in Model 3 could be required to issue a token for EACH AND EVERY RDS query their requestors make*. The TSG must explain this possibility better. This possibility could make multiple queries slow and difficult. But automated queries, at some volume, are essential for Internet security and anti-abuse functions.

Readers must be able to understand the particular way that the TSG is defining the Identity Provider role, and Providers must be able to understand what their role might involve.

POLICY

Unfortunately the TSG's "Draft Technical Model" makes a number of out-of-scope policy recommendations, which the TSG is not situated to make. The TSG should re-cast or remove such

[1] The Requestor sends a query to ICANN's gateway, which then queries s the registry or registrar RDAP sever, the reply goes to the ICANN gateway, and from there back to the requestor.
[2] Per the proposed implementation in Section 9, a query must go from the Requestor to an Identity Provider, which provides a token back to the Requestor, the Requestor then uses the token to query ICANN's gateway, which queries the registry or registrar RDAP sever, the reply goes back to the ICANN gateway, and from there the reply is routed back to the requestor.

recommendations. The TSG was presented to the ICANN community as a technical exercise with narrow remit. It is important for the TSG to hew to its limited scope, since:

1) the TSG is not to overlap with policy-making activities, notably the remit of the ePDP. And,
2) the TSG is a closed group with a membership chosen not by the community but by a chair designated by the ICANN CEO.

The TSG assigned a complex policy-driven role to the Identity Providers, although it may not be necessary to do so.

The need for mandatory Third Party Authorizers will be a policy decision made in the ePDP. But the TSG recommends a solution in which Third Party Authorizers are required (section 9.1), with little technical justification.

Another example of a policy recommendation is **8b**, which states that "ICANN, Identity Providers, and Third Party Authorizers MUST undergo an annual security audit by a third-party auditor and provide the audit report as requested by the interested parties." That is a policy, legal, and contractual recommendation, and is not required to answer to any of the "Key Questions" in the TSG's charter.

The purpose of the TSG's recommendation here is to protect personal data. The data is held primarily by the registries and registrars. But ICANN's contracted registries and registrars have never been required to undergo security audits covering how they handle personal data, or other sensitive data such as credit card data. (And certainly not *annual* audits that must be *released* to "interested parties.") For security and consistency across the environment, the TSG would need to recommend that transparent security audits also be required of all registries and registrars.

Another out-of-scope recommendation is **8d**: "There SHOULD be a mechanism for reporting breaches of data privacy and security (for instance, to be in compliance with Article 33 of the GDPR)." This has nothing to do with a technical implementation -- it is a policy, and would likely use an out-of-band procedure. It's an issue for the ePDP. (And oddly, the TSG states that compliance with GDPR is a SHOULD, not a MUST.)

Other out-of-scope policy recommendation are in **6C** and **10.7**.

The TSG's "Unified Requirements" document also contains scope problems. For example its section 6c says: "The query logs SHOULD NOT be publicly available." That SHOULD NOT means there may be cases for public disclosure. But whether the logs could ever become public under any circumstance is a policy and legal decision and should be referred to policy makers instead.

In other places, the TSG properly avoided the kind of policy specifics noted above. An example is 10.1, where the TSG properly raised an issue for policy-makers to consider.[3] It is unclear why the TSG scrupulously avoided policy pronouncements in some places but not others. The TSG should have been consistent in its approach.

[3] 10.1: "The TSG believes that policies regarding retention and deletion of these data, which are outside of the TSG's narrow technical scope, SHOULD be established, communicated to the data processors, audited and enforced."

USER NEEDS

The TSG has under-examined the needs of requestors and how they will use the system. *The requestors are the main users of the system, for whom RDS services are designed and for whose benefit they are maintained.*

The TSG was well-constituted to understand the needs of the *suppliers* of the data – the registries and registrars. Of the TSG's ten members, six work for ICANN contracted parties. The six included employees of the largest registry operator (Verisign), the second-largest registry operator (Afilias), and the largest registrar (GoDaddy).[4] Only one TSG member was primarily on the *requestor* side (Facebook).

As described above, the TSG assigned a complex operational, transactional, and technical role to the Identity Providers, although it may not be necessary to do so. The TSG's proposal may make it more difficult for communities with legitimate interests in the RDS data to get access. And the TSG's recommendations introduce additional points of failure and possibly slower performance, as mentioned above.

Other examples where the needs of requestors were not given adequate consideration:

1. Section 7a states that "There MUST be SLA commitments for all the service subsystems (e.g., ICANN RDAP Gateway, contracted parties RDAP servers, identity providers, authorizers) availability, and request resolution times." This is important, *but the paper does not state the more fundamental, underlying requirement: that requestors rely on the data for vital uses, sometimes at scale, and the ICANN RDAP gateway MUST be highly available and very fast.* It is not enough to have an "SLA commitment" -- that commitment could be a slow one, with significant downtime. What is important to state is that there must the SLAs that are responsive to the needs of the users.[5] Unfortunately the words "speed," "fast," or "responsive" do not appear the draft paper at all.
2. In SAC101, ICANN's SSAC explained the problems caused by inadequate access to the data, such as the problem of RDS rate limits imposed by operator practices and by inadequate system provisioning. The TSG has not addressed the problems raised in SAC101.
3. The TSG acknowledges that "supporting bulk queries and replies" should not be precluded, but did not given thought to how bulk queries might be supported. And how does the TSG define "bulk" queries – a large number of serial requests, or one request that yields multiple returns?
4. The TSG's "Unified Technical Requirements" states that "The system must be able to process both unauthenticated and authenticated requestors." Can the TSG explain this? The ICANN gateway is designed specifically to serve permissioned users. Unauthenticated users should not receive registration data from the ICANN gateway. Unauthenticated requestors should use the publicly available RDS servers. They could be referred to those distributed sources by ICANN's gateway, but that's probably a policy decision, since referrals will impact system performance and increase the cost of the gateway system.

[4] One additional TSG member works for a numbers registry, and one additional member works for a cert company after having left Verisign in 2018.

[5] Various bodies including law enforcement agencies, the SSAC, M3AAWG, and the Anti-Phishing Working Group have all explained how fast, available, reliable RDS service, performed at scale, is essential for Internet security.

5. Section 9.2 says that "a requestor who wishes to submit an RDAP query must submit an Access Request." RDAP is a stateless protocol, so a separate Access Request will evidently be required for every single query that requestors make? This may add a burden to ICANN's gateway, and to the registries' and registrars' RDAP servers, and will need to be addressed in the SLAs. If there's a way touse session authentication or stateful connections, that might that be helpful.