ICANN org Feedback: Requested Enhancements to Proposed WHOIS Disclosure System

28 October 2022

Executive Summary

This memo assesses three enhancements to the proposed WHOIS Disclosure System that have been requested by the community and the expected impact on costs and timeline, as set out in further detail below

1. **Logging request data for requests associated with non-participating registrars**: ICANN org believes that the WHOIS Disclosure System could collect and retain responses to "pick list" questions submitted by requestors for domains managed by non-participating registrars. The system could also collect free-text responses to the "domain name subject to the request" and "other applicable law (non-GDPR) legal basis" questions. The system should not collect any other free-text answers or attachments. ICANN org did not identify any additional cost or timeline impact related to the addition of this feature.

2. **Transmission of request data to registrars via email:** Request data could be transmitted to participating registrars via encrypted email, provided an adequate encryption key management process is designed. Adding this feature to the WHOIS Disclosure System is estimated to add an additional 2 months of development time and associated staff costs. There would be no additional external costs.

3. **Registrars bulk updates:** A system feature can be added to enable registrars to update the status of requests in bulk in the Naming Services portal. ICANN org did not identify any additional cost or timeline impact related to the addition of this feature.

Detailed Feedback

1. Logging Request Data for Requests Associated with Non-Participating Registrars

ICANN org has been asked to assess whether it would be possible to log information about all attempted requests in the system (even requests attempted for "non-participating" registrars), which would involve recording specific data fields through the Data Request Form of the WHOIS Disclosure System.

From a functionality and user experience perspective, the WHOIS Disclosure System could permit a requestor to continue filling in the complete form. This could enable the requestor to download a copy of the pre-formatted request that they could forward to the non-participating registrars. In this scenario, upon attempting to submit a request to a non-participating registrar, the requestor could be presented with two options:

- Option 1: “I wish to continue filling the form and download the completed form in a standard format.”
- Option 2: “I wish to end the process here.”

The requestor would be presented with a notice that if they select option 1, the system would not send the request to the registrar because the registrar is not participating in the system. The answers submitted to the form’s questions would be retained in the system for statistical purposes only, and would not be associated with the requestor’s ICANN Account data. The benefit to the requestor of continuing to answer the request questions would be that the requestor could download and use the pre-formatted request form to send the request directly to the registrar, which could facilitate the registrar’s review of the request. The purpose for retaining this data in the system would be to inform future decisions about how to proceed with SSAD policy recommendations. The requestor would be provided with a link to more detailed information available in the Privacy Notice.

This data would not be available to the registrar in the system, even if the registrar decides to participate at a later stage.

<u>Assessment: Some Answers Could Be Logged</u>
ICANN org believes that the system could log a subset of “full request” data provided by requestors for names sponsored by non-participating registrars, as set out below, at a low risk for data subjects:

- Date and time stamps for the request (automated by the system)
- Request category (**Q1** - “l*aw enforcement, security researcher, computer security incident response team (CSIRT), cybersecurity incident response team (non-CSIRT), consumer protection, research (non-security), domain investor, IP holder, dispute resolution service provider, litigation/dispute resolution (non-IP), other”*)
- Party representation (**Q5** - “*I am authorized to act on behalf of a third party in submitting this request” or “I am submitting this request on my own behalf”*)
- Jurisdiction where the nonpublic registration data will be processed (**Q7**)
- Domain name subject to the request (**Q8 -** *Note that however this may constitute personal data and it would be useful to identify and document the purpose and the related benefits of collecting this data*)
- Registrar name associated with the domain subject
- List of elements requested (**Q9** - *“Registry Domain ID, Registry Registrant ID, Registrant Name, Registrant Org, Registrant Street, Registrant City, Registrant Postal Code, Registrant Phone, Registrant Email, Tech ID, Tech Name, Tech Phone, Tech Email”*)
- Priority level (**Q10** - Priority 1, 2, and 3, as defined in the request form)
- If Priority 1, the specific circumstance that applies (**Q11** - “*imminent threat to life, imminent threat of serious bodily injury, imminent threat to critical infrastructure, imminent threat of child exploitation*”)

- If Priority 2, the specific circumstance that applies (**Q12** - *"UDRP verification request, URS verification request"*)
- Whether a Law Enforcement request for data such as subpoena, court order, warrant or any other form of legal request been issued requesting the disclosure of the requested data (**Q14** - "*Yes/No*")
- Whether the requestor is asserting a legal basis under which they would process the requested data pursuant to the European Union General Data Protection Regulation or other applicable law? (**Q16** "*Yes/No*")
- If yes to the question 16 above, the legal basis (**Q17** "*GDPR Art. 6(1)a, data subject consent; GDPR Art. 6(1)b, contractual necessity; GDPR Art. 6(1)c, compliance with a legal obligation to which the controller is subject; GDPR Art. 6(1)d, processing is necessary to protect the vital interests of a data subject or other natural person; GDPR Art. 6(1)e, processing is necessary for a task carried out in the public interest, as set out in EU or EU Member State law; GDPR Art. 6(1)f, legitimate interests; other applicable law (non-GDPR) legal basis")*
- If 'other' is selected in question 16 above, the applicable law identified including a section reference and explanation (**Q18** - *Note that however this is free text and there could be a moderate risk of having personal data included*)

Recommendation: No Logging of Most Free-Text Fields or Attachments

Data request form answers that are likely to contain personal and potentially other confidential data (such as answers explaining requests submitted in relation to alleged crimes), with free text (except question 18 mentioned above), and attachments should not be recorded in the WHOIS Disclosure System. Collection of these responses would pose an undue risk related to the collection and retention of such data, without a clear countervailing benefit. It is unclear how the collection and retention of this data would be useful to understand usage of the WHOIS Disclosure System or to further community discussions concerning the recommendations for an SSAD.

These request form questions are:

- Description of the request category (the specific capacity in which the requestor is submitting this request) if "other" is selected (**Q2** - free text)
- Additional contact details: Postal Address (**Q3** - personal data)
- Additional contact details: telephone number (**Q4** - personal data)
- Attachment of power of attorney from the party represented if Q5 is selected (**Q6** - attachment which will likely contain personal data)
- Brief description of the specific issue the request is attempting to resolve (**Q13** - free text)
- Specific date by which the contracted party must respond and attach a copy of the Law Enforcement request (**Q15** - deadline is not relevant for statistical purposes and attachment)
- Attach any relevant documentation in support of the request, including any Law Enforcement request (subpoena, court order, etc.) (**Q19** - attachments)

ICANN org did not identify any additional cost or timeline impact related to the addition of this feature.

2. Transmission of Request Data to Registrars via Email

The community has asked whether the email notifying a participating registrar of a request could contain all the information required to act upon the request, allowing the registrar to process the request without the operational overhead of having to log into the NSP.

Based on this request, ICANN org considered 3 alternatives: (a) sending request data by simple (unencrypted) email; (b) sending non-personal and non-confidential data (e.g. the request fields identified above in the "fields that could be logged"); and (c) sending the completed data request form via encrypted email.

Options (a) and (b) do not appear to be viable solutions. Option (a) would pose a data protection and security risk, and option (b) would not provide the functionality the registrars are seeking (since they would still need to log into the portal to view full request data).

Option (c) (sending requests via encrypted email) appears to be an appropriate solution. Encryption is generally recognised as an appropriate technical measure to ensure personal data (and data in general) is processed securely and to mitigate the risks of data interception. The method currently envisaged for email encryption is PGP (Pretty Good Privacy) keys. The PGP keys are used to encrypt texts, emails, signing files, etc. PGP keys work as a key pair as they have a public key and a private key. Registrars will provide their public PGP key and ICANN org will use it to encrypt the emails (on a per registrar basis). The registrars will hold the private key. ICANN org advises that if the completed Data Request Forms would be sent via email, these emails would need to be encrypted to mitigate the risks identified related to email communication. An adequate encryption key management process will need to be designed.

To support the encrypted email and attachments feature request the following capabilities must be added to the design:

- A means for Salesforce to encrypt request form content using PGP encryption;
- A secure means of easily downloading attachments (without having to login into NSp);
- Public key management: Registrars would need to upload their active public keys and manage the key lifecycle.

Registrars will be responsible for managing their keys and ensuring a valid key has been uploaded. In the event of a problem with the keys, the system will cease sending encrypted emails to that registrar. ICANN org would need to discuss further with registrars and the GNSO Small Team the impact of a registrar not maintaining their public keys.

The Small Team has also asked about the possibility of creating an API for transmitting request data to the registrars, and for registrars to transmit data concerning actions taken on such requests back to the

WHOIS Disclosure System. It is expected that this would not occur in the initial rollout of a WHOIS Disclosure System based on ICANN org's meeting with select registrars on 14 October 2022, so this is not analyzed in detail in this memo.

The total impact for this feature is estimated to be an additional 2 months of development time and associated staff costs. There would be no additional external costs. Registrars would be responsible for managing their own keys. ICANN org does not plan to validate or force key rollover if a key is expired. User questions and difficulties may arise in the course of key management. ICANN org is prepared to operationally support this service in order to improve the registrar experience and thus increase participation. It is challenging to estimate the number of participating registrars as well as the number and nature of support requests. Whatever the volume, there will be an impact on ICANN's operations, which may increase costs. Once the implementation details related to the key management mechanism are determined, an additional impact assessment will be conducted to determine if there are any additional cost or time implications.

3. Registrars bulk updates

Although this was not specifically asked as a Minimally Viable Product feature, ICANN org heard from some registrars that this will ease the registrar's manual work when reporting disclosure decisions. ICANN org explored the feature and mocked up a registrar interface for bulk updates, which allows registrars to select multiple pending requests to provide updates in a list view. ICANN org is prepared to demonstrate this feature for the Small Team, at their request. ICANN org did not identify any legal concerns, or cost or timeline impact related to the addition of this feature.