

# **Expert Working Group on gTLD Directory Services (EWG) | Frequently Asked Questions (FAQs)**

## **Origin and Purpose of the EWG**

1. What is the Expert Working Group (EWG)?
2. Who are the members of the EWG?
3. What is the EWG's objective? How does it differ from the WHOIS RT?
4. What is the EWG expected to produce and when?

## **Origin and Purpose of the RDS**

5. What is the next-generation gTLD Registration Directory Service (RDS)?
6. Why is a next-generation RDS really needed?
7. What makes the RDS fundamentally different from today's WHOIS?

## **Registration Data Users and Purposes**

8. Who are the users of the RDS? How did the EWG determine this?
9. Why do those users need access to registration data?
10. Which purposes should not be permissible?
11. Why didn't the EWG consider user X or purpose Y?

## **Registration Data Elements**

12. What registration data should be collected and stored by the RDS?
13. Why is the RDS only concerned with gTLD registration data?
14. How would RDS data differ from WHOIS data?
15. Would the RDS collect the same registrant data for domains used for commerce?
16. When and how would a data risk assessment be performed?

## **Registration Data Collection and Storage**

17. What roles do registrars, registries and the RDS play in data collection and storage?
18. What data would be mandatory to collect/store?
19. How long would data be stored by the RDS?

## **Purpose-Driven Data Access and Disclosure**

20. What is purpose-driven registration data access?
21. Does the RDS eliminate free public access to registration data?
22. Who would have gated access to registration data and what would it cost?
23. What would deter abuse of gated access?
24. Would registrars and registries still be able to provide direct access?

## **Addressing Registration Data Privacy Concerns**

25. Would privacy and proxy services still exist in the RDS? How would they differ?
26. How would the RDS accommodate the personal data privacy needs of at-risk registrants?
27. What would prevent insider abuse or external hacking of RDS data?
28. How would the RDS comply with local data protection laws?

## **Addressing Registration Data Accuracy Concerns**

29. Why would RDS data be any more accurate than today's WHOIS data?
30. How and when would the RDS validate registration data?
31. Wouldn't registrars and registries still have to validate data?
32. How would the RDS deal with inaccurate registration data?
33. What is pre-validation and how would it help improve accuracy?

## **Addressing Registration Data Accountability Concerns**

34. Would the RDS offer greater accountability for anonymous public data access?
35. How would credentials be issued for gated access?
36. Who would decide which requestors should have access to which data elements?
37. How would the RDS hold requestors accountable for use of data obtained via gated access?

## **Suggested Model and Benefits/Limitations**

- 38. Why did the EWG suggest an Aggregated RDS model?
- 39. What are the primary benefits of the ARDS model?
- 40. Doesn't the ARDS model elevate risk of abuse and attack?
- 41. What other models did the EWG consider? Why weren't they chosen?

### Impacts and Costs

- 42. What would the RDS cost to build and who would pay for it?
- 43. Would registrant's costs increase?
- 44. Would requestor's costs increase?
- 45. In what ways would the RDS likely reduce cost?

### Next Steps

- 46. What will the EWG do with comments on its draft report?
- 47. When will the EWG produce its final report?
- 48. What will be done with the EWG's final report?

## **Origin and Purpose of the EWG**

1. What is the Expert Working Group (EWG)?  
The [EWG](#) was formed by ICANN's President & CEO, at the [request of ICANN's Board](#), to help resolve deadlock within the ICANN community on how to replace the current WHOIS system with a next-generation gTLD directory service that better meets the needs of today's & tomorrow's Internet.
2. Who are the members of the EWG?  
The EWG is comprised of [13 volunteers](#), selected from over 70 applicants to use their diverse experiences, perspectives and expertise to help solve the problem. The group is guided by lead facilitator, Jean-Francois Baril, and includes two liaisons from the ICANN Board.
3. What is the EWG's objective? How does it differ from the WHOIS RT?  
Unlike past efforts to fix WHOIS, the EWG started with a clean slate, questioning fundamental assumptions about the purposes, uses,

collection, maintenance and provision of gTLD registration data, as well as accuracy, access, and privacy needs.

4. What is the EWG expected to produce and when?

The EWG hopes to publish its Final Report by October for delivery to ICANN's CEO and Board to serve as a foundation for new gTLD consensus policy development, and contractual negotiations, as appropriate.

### **Origin and Purpose of the RDS**

5. What is the next-generation gTLD Registration Directory Service (RDS)?

The [RDS is a proposed successor for today's WHOIS](#) that would collect, validate and disclose gTLD registration data for permissible purposes only, with some data elements accessible only to authenticated requestors that are then held accountable for appropriate use.

6. Why is a next-generation RDS really needed?

The WHOIS system is over 25 years old and has not kept pace with the evolution of the global Internet. After more than 12 years of task forces, working groups, and studies, concerns about WHOIS data access, accuracy and privacy remain unresolved.

7. What makes the RDS fundamentally different from today's WHOIS?

The RDS takes a clean-slate approach, abandoning one-size-fits-all WHOIS in favor of purpose-driven access to validated data in hopes of improving privacy, accuracy and accountability.

### **Registration Data Users and Purposes**

8. Who are the users of the RDS? How did the EWG determine this?

The EWG analyzed previous reports and use cases to identify users who want access to gTLD registration data, including registrants, protected registrants, on-line service providers, business Internet users, intellectual property owners, law enforcement agencies and OpSec staff, Internet technical staff, individual Internet users, researchers, non-LEA investigators of malicious activity and bad actors.

9. Why do those users need access to registration data?  
Use cases also shed light on rationale and purpose served by gTLD registration data, including domain name control, regulatory/contract enforcement, domain name research, domain name purchase/sale, personal data protection, individual Internet use, technical issue resolution, Internet services provision, legal action, abuse mitigation and malicious Internet activities.
10. Which purposes should not be permissible?  
Given no rationale for accommodating the needs of some users but not others that access WHOIS today, the EWG recommended the RDS accommodate all non-malicious uses.
11. Why didn't the EWG consider user X or purpose Y?  
Use cases examined by the EWG were not exhaustive, but representative enough of existing and potential uses to establish RDS needs. Community input is solicited on important gaps.

## **Registration Data Elements**

12. What registration data should be collected and stored by the RDS?  
The EWG also analyzed use cases to identify data needs. The draft report summarizes existing and potential RDS data elements, mapped to purposes. Comment is solicited on important gaps.
13. Why is the RDS only concerned with gTLD registration data?  
The EWG was tasked with making recommendations to inform gTLD policy-making, but has also examined ccTLD WHOIS to inform RDS principles, many of which are meaningful for any TLD.
14. How would RDS data differ from WHOIS data?  
Unlike WHOIS data, RDS data would be validated at the time of collection and periodically by applying standard checks. The RDS may also collect some data elements identified as desired to fully-address identified purposes, but not generally presented through WHOIS today.
15. Would the RDS collect the same registrant data for domains used for commerce?  
The EWG intends to continue its work in this area, but some potential new data elements (e.g., Domain Name Purpose, Registrant Company Identifier) have already been identified to more clearly identify domains used for commerce and legal person registrants.

16. When and how would a data risk assessment be performed?

The EWG expects to derive initial recommendations but recommends that risk analysis be performed on each data element. Comment is requested on how this risk analysis should be conducted, who should conduct it, and criteria by which each data element should be classified.

### **Registration Data Collection and Storage**

17. What roles do registrars, registries and the RDS play in data collection and storage?

In the suggested model, registrars continue to collect and maintain data from their customers (registrants), while registries continue to store gTLD data collected from their customers (registrars) as done for "thick WHOIS." The RDS is not involved in data collection, but uses an aggregate copy to provide uniform validation and access for all gTLD registration data.

18. What data would be mandatory to collect/store?

The EWG recommends that only data elements with at least one permissible purpose be collected by the RDS. Identified data has yet to be categorized as mandatory or optional.

19. How long would data be stored by the RDS?

The EWG asks for community input on needs that should be considered during its discussion of registration data storage duration, escrow and access log requirements.

### **Purpose-Driven Data Access and Disclosure**

20. What is purpose-driven registration data access?

The RDS introduces *purpose-driven data access*, which provides gated access to data based on a requestor's identity and stated purpose. Only authenticated requestors authorized for a given purpose (and held accountable to terms and conditions) can access associated data elements.

21. Does the RDS eliminate free public access to registration data?

No. The EWG recommends that anonymous public access to an identified (non-null) minimum data set be made available, with

restrictions to limit bulk harvesting. This public access to basic registration data should satisfy many Internet user needs.

22. Who would have gated access to registration data and what would it cost?

The EWG recommends that gated access processes should create a level playing field for all requestors with the same purpose. The EWG expects to discuss specific processes for gated access by accredited Law Enforcement Agencies and other licensed requestors (e.g., IP Owners).

23. What would deter abuse of gated access?

The RDS would log and audit public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use. Different terms and conditions may be applied to different purposes. If requestors violate terms and conditions, penalties would apply.

24. Would registrars and registries still be able to provide direct access?

To enable authentication, access control, and accountability, all public access to gTLD registration data would occur through the RDS. However, this would not impede other registrar and registry data interactions with their own customers.

### **Addressing Registration Data Privacy Concerns**

25. Would privacy and proxy services still exist in the RDS? How would they differ?

The EWG recommends there be accreditation for privacy/proxy service providers and rules regarding provision and use of accredited privacy/privacy services. Principles are still being developed, including processes to meet the needs of Law Enforcement.

26. How would the RDS accommodate the personal data privacy needs of at-risk registrants?

One possible option to accommodate at-risk registrant needs for "secure protected credentials" is for ICANN to accredit an independent organization to act as a Trusted Agent that, using a set of agreed criteria, would determine whether a registrant qualified for this maximum protection. Comments are requested on how a suitable solution might be identified and funded.

27. What would prevent insider abuse or external hacking of RDS data?  
Proper system design, security measures, audits and oversight would be needed to minimize data breach risk. Insider abuse should be deterred through security policy, implementation, enforcement and third-party auditing.
28. How would the RDS comply with local data protection laws?  
The EWG recommends that policies should be established by each RDS stakeholder participating in data access, use, retention and due process. These policies may vary depending upon the jurisdiction and must enable compliance with local laws.

### **Addressing Registration Data Accuracy Concerns**

29. Why would RDS data be any more accurate than today's WHOIS data?  
The EWG proposes more robust validation of registrant data than the [2013 RAA](#). In addition, with gated access to more sensitive data elements, registrants would have less incentive to supply inaccurate data, coupled with more accountability for ensuring data accuracy.
30. How and when would the RDS validate registration data?  
The RDS would apply standard validation to all gTLD registration data. In addition to periodic checks, validation would occur at time of collection, with an option to pre-validate registrant contact data for reuse in multiple domain name registrations.
31. Wouldn't registrars and registries still have to validate data?  
Registrars would still be accountable to provide service to registrants as specified in their contracts, including ensuring provision of current, accurate registration data. However, a standard validation service could make this more efficient by routinely performing syntactic and operational validation and notifying registrars of inaccuracies, for example.
32. How would the RDS deal with inaccurate registration data?  
The RDS would hold registrants accountable for providing and maintaining current, accurate and timely registration data. The EWG expects to further explore processes and repercussions.
33. What is pre-validation and how would it help improve accuracy?  
To improve accuracy and reduce fraud, registrants could optionally supply a globally-unique name/organization and associated details



prior to first domain name registration. Once "pre-validated" for accuracy and uniqueness, that registrant (and only that registrant) could maintain and associate that data with many domain names.

### **Addressing Registration Data Accountability Concerns**

34. Would the RDS offer greater accountability for anonymous public data access?

Yes, to some degree. The RDS would log all access to gTLD registration data, including anonymous public data access, with restrictions to deter bulk harvesting.

35. How would credentials be issued for gated access?

Gated access would only be available to requestors who applied for and were issued credentials for RDS query authentication. The EWG does not expect to define the specific process by which the RDS operator would issue access credentials.

36. Who would decide which requestors should have access to which data elements?

The EWG has identified data needs for each identified user/purpose, but recommends that risk analysis be performed on each data element to inform access policy. Comment is requested on how this risk analysis should be conducted and who should conduct it.

37. How would the RDS hold requestors accountable for use of data obtained via gated access?

The RDS would log and audit public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use. Different terms and conditions may be applied to different purposes. If requestors violate terms and conditions, penalties would apply.

### **Suggested Model and Benefits/Limitations**

38. Why did the EWG suggest an Aggregated RDS model?

The Aggregated RDS (ARDS) model was suggested as one beneficial way of addressing the desired features and principles recommended to satisfy identified users and their data needs.

39. What are the primary benefits of the ARDS model?

Benefits of this model include "one stop shopping" for requestors,

greater accountability, ability to track/audit data and access across TLDs, ability to support enhanced search capabilities, opportunity to minimize some costs, support for requestor validation/accreditation, opportunity for more efficient accuracy management, and opportunity for internationalized web portal.

40. Doesn't the ARDS model elevate risk of abuse and attack?

As a "Big Data" source of highly valuable data, there is clearly potential for attack or abuse if not properly secured, audited and maintained. However, this risk may be no greater than risk posed by a highly distributed model with inconsistent and less easily-audited security measures.

41. What other models did the EWG consider?

In reaching consensus on the ARDS model, the EWG considered the Zone File Advisory Group's analysis. With thousands of new gTLD registries, a distributed model would create inefficiencies, escalate costs, and complicate problem resolution. Distributed or proxy models also could not easily accommodate commonly needed features such as a cross-TLD registrant look-up.

## **Impacts and Costs**

42. What would the RDS cost to build and who would pay for it?

Recognizing that GNSO policy decisions and Staff implementation actions ultimately will determine the cost, the EWG plans to explore this important issue further at a high level to inform these future efforts. Elements to be explored include potential costs of development and operation and possible ways in which these might be borne (e.g., absorbed by RDS funding, offset by value-added service fees). Community input on impacts and costs is requested.

43. Would registrant's costs increase?

The EWG recommends that the RDS operate on a cost-recovery basis, with the goal of minimizing total cost to the entire ecosystem through greater efficiency. At this point, it is impossible to determine if the nominal cost of registering a domain will change, but the RDS should reduce many of the "hidden costs" that registrants bear today.

44. Would requestor's costs increase?

The EWG acknowledges that some aspects of the proposed model

will incur new costs, but believes that many other hidden costs incurred with today's inefficient and too-often-inaccurate WHOIS system will be reduced. As the proposed RDS delivers new and improved services, both benefits and costs must be evaluated. The proposed approach will provide policy-makers the option, for the first time, to craft ways for those requesting registration data from the system to efficiently contribute to the operation of that system.

45. In what ways would the RDS likely reduce cost?

The proposed RDS will reduce cost in many ways, including more scalable and efficient validation, reduced fraud, improved accuracy, reduction in inaccuracy complaints, reduced personal privacy risk to registrants, efficiencies gained through automation, and faster time-to-resolution for all requestors using RDS.

## Next Steps

46. What will the EWG do with comments on its [draft report](#) [PDF, 1.7 MB]?

[All input received by 12 August](#) on the report and [discussion questions](#) [PDF, 73 KB] will be used to inform the EWG as it refines its recommendations, completes open areas and finalizes its report.

47. When will the EWG produce its final report?

The EWG hopes to publish its final report in October, before the Buenos Aires ICANN meeting, subject to confirmation after the draft comment period closes.

48. What will be done with the EWG's final report?

The EWG's final report will be published and delivered to ICANN's CEO and Board to serve as a foundation for the Board-requested GNSO Policy Development Process (PDP) for the provision of gTLD registration data and contractual negotiations, as appropriate.