Request for Information - Registration Directory Service (RDS) User Accreditation

10 February 2014

Internet Corporation of Assigned Names and Numbers Request for Information

1.0 Introduction

1.1 About this Document

By issuing this Request for Information ("RFI"), the Expert Working Group on Next Generation gTLD Directory Services ("EWG"), convened by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is requesting information about organizations capable of accrediting users of the new Registration Directory Service (RDS) now under consideration to replace the current WHOIS system. RDS users may include (but are not limited to) Registrants, Proxy Service Providers and Customers, Internet Technical Staff, On-Line Service Providers, Individual and Business Internet Users, Internet Researchers, Intellectual Property Owners, Law Enforcement Agencies, Operations/Security Incident Investigators, and others requesting gTLD domain name registration data for legitimate purposes.

1.2 Overview of ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation responsible for coordinating critical Internet resources. These include Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain Name System (DNS) management, and root server system management. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

In support of this mission, ICANN develops policy for WHOIS services that provide public access to data about registered domain names. The extent of data collected at the time of domain name registration, and the ways such data can be accessed, are specified in agreements established by ICANN for domain names registered in gTLDs.

For example, ICANN currently requires accredited registrars to collect and provide free public access to information about each registered gTLD domain name, including the name servers for that domain, the date the domain was created and when its expires, the Registered Name Holder's name and contact information, and designated Technical and Administrative contacts. Today, anyone can obtain this data by using the WHOIS system.

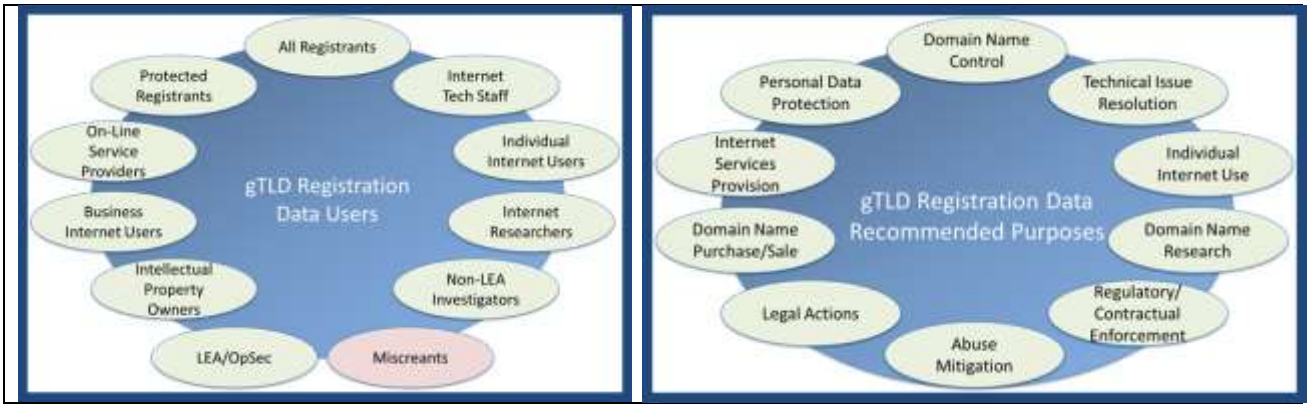
In 2013, the Expert Working Group on gTLD Directory Services (EWG) was formed by ICANN's CEO, Fadi Chehadé, at the request of ICANN's Board, to help resolve the nearly decade-long deadlock within the ICANN community on how to replace the current WHOIS system. The EWG's mandate is to reexamine and define the purpose of collecting and maintaining gTLD registration data, consider how to safeguard and improve accuracy and access to that data, and propose a next generation solution that will better serve the needs of the global Internet community.

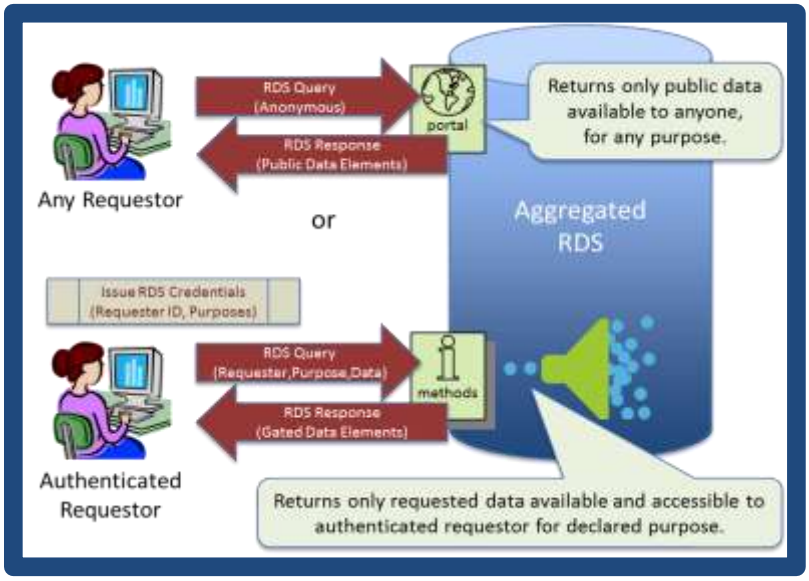
Please see www.icann.org/en/groups/other/gtld-directory-services for more information on the EWG's recommendations for gated access to registration data by accredited users with permissible purposes.

1.3 Overview of the Initiative

The EWG is working to complete its recommendations, including principles to better safeguard the data that users can request from the next-generation Registration Directory Service (RDS). After working through a broad array of use cases, and the myriad of issues they raised, the EWG concluded that today's Whois model—giving every user the same anonymous public access to gTLD registration data—should be abandoned. Instead, the EWG recommended a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data remaining public and other data being gated – that is, returned only to accredited users that are held accountable for appropriate use.

In its Initial Report, the EWG drafted a set of actual use cases involving the Whois system, analyzing each case to identify (i) the users who want access to data, (ii) their rationale for needing such access, (iii) the data elements they need and (iv) the purposes served by such data. These users, purposes, and their authenticated access to registration data through the RDS are summarized in the following figures.





The EWG is still working to flesh out several key areas, including principles for RDS user accreditation – that is, processes by which gTLD registration data users might apply for and be issued credentials enabling access to gated data elements. The information gathered by this RFI will to inform the EWG's deliberations as it finalizes its recommendations for this crucial area.

The EWG is releasing this Request for Information to solicit responses from organizations that currently issue system access credentials to authorized members of their own community, using defined acceptance criteria. For example:

- Law Enforcement Agencies may vet and train Law Enforcement Officers before issuing credentials that can be used to authenticate and gain access to restricted areas or systems;
- Internet Security Firms may issue credentials to legitimate OpSec Investigators, for use in accessing sensitive data obtained from cyber threat databases and live event feeds; and
- Numerous industry trade associations issue credentials to their memberships to enable access to password-protected websites and events.

These are just a few examples of organizations that might wish to respond to this RFI, describing existing accreditation practices applied to a user community that may also need access to gated registration data.

At this juncture, the EWG wishes to identify organizations that today issue credentials to communities identified as gTLD registration data users in the above figures, or any other communities that may have a definable purpose for accessing gated data. The EWG hopes to build upon existing membership or credentialing processes to fulfill RDS user accreditation needs, should ICANN pursue RDS implementation.

Following a GNSO policy development process (PDP), to be commenced at the Board's request to evaluate the EWG recommendations, the ICANN Board may or may not decide to fund development of a next-generation RDS, and may or may not issue a Request for Proposal (RFP) seeking bids from organizations wishing to be awarded responsibility for accrediting RDS users.

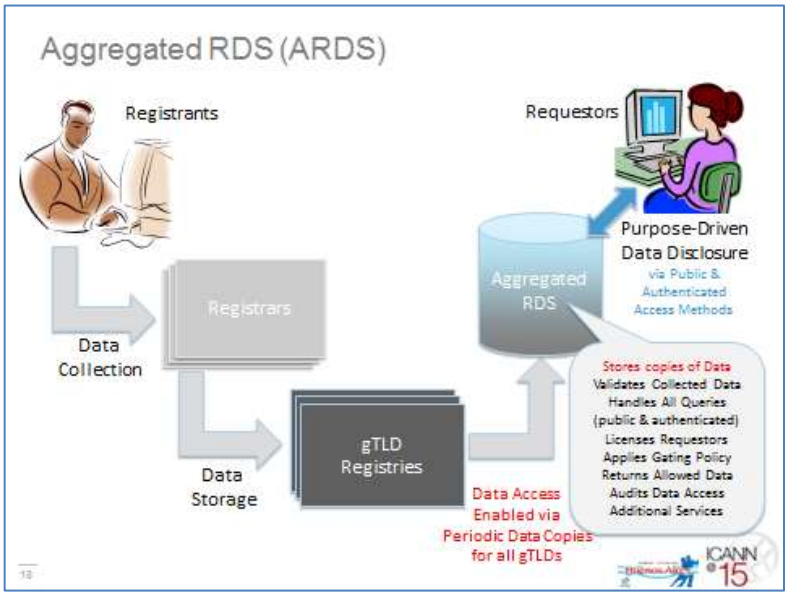
As the purpose of this RFI is purely informational – that is, to inform the development of policies and procedures -- potential Respondents responding to the future RFP (if any) will not be bound by the estimates, prices, or other information provided in response to this RFI. Similarly, there is no obligation on the part of parties responding to this RFI to submit a future RFP bid, or for ICANN to proceed to RDS implementation, with or without issuing a future RFP.

Section 2.0 Objectives and Requirements

2.1 Objectives

As described in Section 1.3, the EWG has suggested replacing anonymous public WHOIS access with a next-generation RDS that delivers public access to some data and gated access to more sensitive data, depending upon each user's authenticated identity and purpose. Implementing gated access would require processes and policies for applying for RDS access, issuing credentials to accredited users, authenticating gated access requests, and holding users accountable for any misuse of data.

The following figure illustrates one of two system models for a next generation RDS that the EWG has identified as having the potential to fulfil many of the principles discussed in the EWG's Initial Report.



Some key features of this proposed RDS that impact accredited user access to gated data include:

- The RDS serves as an aggregated (centralized) or federated (distributed) repository that contains a non-authoritative copy of data elements collected for each registered domain
- The RDS discloses registration data through defined access methods
    - For consistency, the RDS serves as a central point of access
    - Public data access delivered via anonymous query (e.g., website)
    - Gated data access delivered via other multi-modal access methods (e.g., RDAP)
- The RDS manages licensing arrangements for access to non-public, gated data elements
    - Users who wish to obtain gTLD registration data may apply for RDS access credentials
- To deter misuse and promote accountability
    - RDS access should be authenticated to appropriate level

- Accreditation of requestors needing gated access
- If terms and conditions of access are violated, penalties may be applied

To learn more about the EWG's proposed RDS, watch this short introductory video, listen to this longer presentation, or consult these RDS FAQs. Sections of the EWG's Reports describing RDS users and their purposes, accreditation of RDS users, and public/gated access have been included Appendices of this RFI.

2.2 Required Experience of Potential Respondents

Ideally, ICANN expects that potential Respondents to this RFI will satisfy the following experience requirements:

1. Have a demonstrated ability to identify and enroll members of a given community in an orderly and fair manner, preferably on a regional or global scale.
2. Have a track record in competently handling user enrollment requests, including applicant review, approval/accreditation, and licensing/credentialing.
3. Have a track record in user account lifecycle management, including account creation, update, termination, and enforcement of terms and conditions.
4. Have the ability to scale quickly to meet the demands of an unknown number of new user accreditation requests throughout the world.
5. Have the ability to communicate with and accredit users in multiple languages.
6. Have a demonstrated understanding of audit processes and data protection needs.
7. Have a demonstrated understanding of domain name registration data needs and purposes for a given community.

2.3 RDS Specific Requirements

Potential respondents to this RFI should provide information about their existing relationship to one or more proposed RDS user communities, including:

1. Natural Person Registrants (i.e., individual persons registering a domain name)
2. Legal Person Registrants (i.e., companies or organizations registering a domain name)
3. Proxy Service Providers (i.e., agents registering domain name(s) for use by third parties)
4. Protected Registrants (i.e., customers of a Proxy Service Provider)
5. Internet Technical Staff (e.g., DNS, email, or website administrators)
6. On-Line Service Providers (e.g., ISPs, hosting providers, certificate authorities)
7. Individual Internet Users (e.g., consumers)
8. Business Internet Users (e.g., brand holders, brokers)
9. Internet Researchers
10. Intellectual Property Owners (e.g., trademark owners)
11. Law Enforcement Agencies
12. Operations/Security Incident Investigators
13. Other Investigators (e.g., tax authorities, UDRP providers)
14. Other existing or future users with legitimate needs for gTLD registration data

Organizations that issue access credentials to authorized members of one or more of the above user communities are invited to describe their existing practices and suggest ways in which those practices might be extended to meet the RDS user accreditation requirements detailed in Annex A.

2.4 Information Requested

Responders are encouraged to provide information on any of the following areas:

1. Does your organization currently enroll members and issue data or system access credentials to any of the proposed RDS user communities listed above? If so, please describe:
    a. Your organization's name and legal address
    b. Your organization's mission or charter
    c. Your organization's relationship to the proposed RDS user community
    d. Your organization's geographic reach and membership demographics
    e. Your organization's government or legal authorization (if any)
    f. Your organization's point of contact for follow-up purposes (name, address)

2. Does your organization maintain a membership list, where members must apply to join and applicants are reviewed and approved in some manner? If so, please describe:
    a. Summary description of membership requirements (including fees)
    b. Terms and conditions of membership
    c. Whether applicants can be individuals, organizations, or both
    d. Description of application process, including form and information requested
    e. Description of review/approval process, including acceptance criteria
    f. Whether applicant's identity is validated or references are verified
    g. Description of physical or digital credentials issued to approved users (if any)
    h. Systems or data to which credentialed users are granted access
    i. Specified purposes (if any) associated with membership or access
    j. Typical delay until account is approved
    k. Reasons for rejection and dispute process (if any)

3. Does your organization maintain user accounts for approved members? If so, please describe:
    a. Purpose of user account
    b. Mandatory data and/or access credentials associated with user account
    c. Processes for updating user account data and credentials (e.g., password reset)
    d. Processes for temporarily suspending, revoking, or mutually terminating accounts
    e. Processes for enforcing terms and conditions of membership, including
        i. Steps taken to audit compliance with ToC
        ii. Process to remediate detected or reported ToC violations
        iii. Measures (if any) used to pro-actively deter ToC violations
    f. Reasons for account revocation/termination and dispute process (if any)

4. Does your organization have a formal agreement to partner with other similar organizations, such

that your members are recognized by your partners and vice versa? If so, please describe:

a. Relationship between partner organizations
b. Membership services extended to partner's members
c. Limits or constraints placed on partner's members
d. Process (if any) for federated authentication and system/data access

5. Do you see opportunities to build upon your existing processes to accredit RDS users?
   a. Could your processes help in vetting RDS user applications?
   b. Could your processes help in confirming RDS user identity?
   c. Could your processes help in determining legitimate need to access data?
   d. Could the access credentials that you issue be reused for RDS access?
   e. Could your enforcement and compliance processes be extended to deter RDS misuse?

6. Is there any additional information that should be considered by the EWG as it finalizes its recommendations with respect to RDS user accreditation?

7. What issues or concerns do you foresee with respect to accrediting RDS users listed above?

Section 3.0 Instructions to Respondents

3.1 Definitions

"Respondent" means any person or firm receiving this RFI or submitting a response in response to this RFI.

"RDS User" means any individual or organization requesting access to gTLD registration data using a next-generation Registration Directory Service (RDS).

"RDS User Accreditation" refers to the processes by which gTLD registration data users might apply for and be issued credentials enabling access to gated data elements.

"Gated Access" refers to requests for sensitive registration data elements made available only to users who apply for and are issued credentials for RDS query authentication. Gated access responses depend not only upon the user's authenticated identity, but also stated purpose and requested data elements.

3.2 Timeline for Response

Responses are requested email to: rfi-response@icann.org by the close of business (UTC 23:59) on 10 March 2014.

Annex A - Excerpts from the EWG's Initial Report and Status Update Report

From the EWG's Initial Report:

III. METHODOLOGY - IDENTIFYING USERS AND PURPOSES

3.1 Use Case Methodology

The EWG was encouraged to take a clean slate approach in its efforts to define the next generation of registration directory services, rather than improvements to the current WHOIS system, which is widely regarded as inadequate. Consistent with the Board's directive, the EWG commenced its analysis by examining existing and potential purposes for collecting, storing, and providing gTLD registration data to a wide variety of users.

To accomplish this, EWG members drafted an extensive set of actual use cases involving the current WHOIS system, analyzing each of them to identify (i) the users who want access to data, (ii) their rationale for needing such access, (iii) the data elements they need and (iv) the purposes served by such data. Cases were also used to identify all stakeholders involved in collecting, storing and providing registration data, helping the EWG understand existing and potential workflows and ways in which these users and their needs might be better satisfied by a next generation RDS.

These use cases were not intended to be exhaustive, but rather representative of the many uses of the current WHOIS system, illustrating a wide variety of users, needs and workflows. An inventory of uses cases considered by the EWG is provided in Annex B *[of the EWG's Initial Report]*.

The EWG considered the totality of these use cases and lessons learned from them in order to derive a consolidated set of stakeholders and desirable purposes that should be accommodated by the RDS, as well a set of potential misuses that the system should attempt to deter (further detailed in the next section of this report.)

Moreover, the EWG consulted reference materials from previous WHOIS-related activities, community inputs, and use cases to examine specific needs in each of the areas set forth in Figure 1 below.

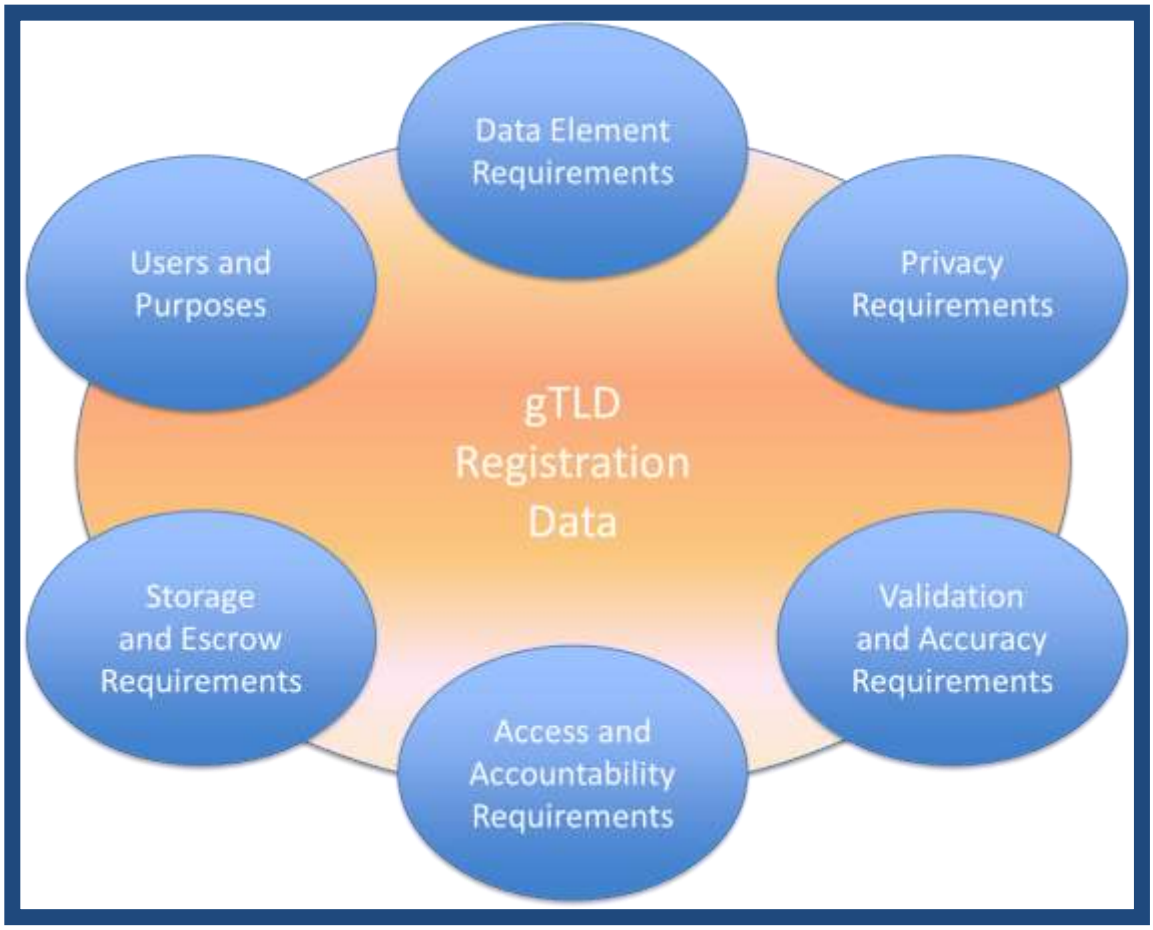


Figure 1: Needs Analysis

The EWG expects to continue its work by analyzing these purposes and needs to derive minimum data elements, related risks, privacy law and policy implications, and additional questions to be more fully explored in the final draft of this report.

3.2 Identifying the Users of the RDS

The EWG analyzed each of the representative use cases to develop the following table, which summarizes the kinds of users who want access to gTLD registration data, the rationale for needing access, and the overall purposes served by that data. Further detail about each use case and user interactions with the RDS is provided in Annex B *[of the EWG's Initial Report]*.

User	Purpose	Example Use Cases	Rationale for registration data access
All Registrants (e.g., natural persons, legal persons, privacy/proxy providers)	Domain Name Control	Domain Name Registration Account Creation	Enable registration of domain names by any kind of registrant by creating a new account with a registrar
		Domain Name Data Modification Monitoring	Detect accidental, uninformed or unauthorized modification of a domain name's registration data

User	Purpose	Example Use Cases	Rationale for registration data access
		Domain Name Portfolio Management	Facilitate update of all domain name registration data (e.g., designated contacts, addresses) to maintain a domain name portfolio
		Domain Name Transfers	Enable registrant-initiated transfer of a domain name to another registrar
		Domain Name Deletions	Enable deletion of an expired domain name
		Domain Name DNS Updates	Enable registrant-initiated change of DNS for a domain name
		Domain Name Renewals	Enable renewal of a registered domain name by the domain name's billing contact (an individual, role or entity)
		Domain Name Contact Validation	Facilitate initial and on-going validation of domain name registration data (e.g., designated contacts, addresses)
Protected Registrants (e.g., customers of privacy/proxy services)	Personal Data Protection	Enhanced Protected Registration	Enable use of accredited privacy or proxy registration services by any registrant seeking to minimize public access to personal names and addresses
		Maximum Protected Registration	Enable use of accredited proxy registration services by individuals or groups under threat, using blind credentials issued by a trusted third party
Internet Technical Staff (e.g., DNS admins, mail admins, web admins)	Technical Issue Resolution	Contact with Domain Name Technical Staff	Facilitate contact with technical staff (individual, role or entity) who can help resolve technical or operational issues with Domain Names (e.g., DNS resolution failures, email delivery issues, website functional issues)
On-Line Service Providers (e.g., ISPs, hosting providers, CAs, reputation services)	Internet Services Provision	Contact with Domain Name Registrant	Enable re-establishment of contact with a customer (individual, role or entity) to deal with business issues for a Domain Name when a provider's usual contact methods fail
		Domain Name Reputation Services	Enable domain name white/black list analysis by reputation service providers
		Domain Name Certification Services	Help a certification authority (CA) identify the registrant of a domain name to be bound to an SSL/TLS certificate

User	Purpose	Example Use Cases	Rationale for registration data access
Individual Internet Users (e.g., consumers)	Individual Internet Use	Real World Contact	Help consumers obtain non-Internet contact information for domain name registrant (e.g., business address)
		Consumer Protection	Afford a low-key mechanism for consumers to contact domain name registrants (e.g., on-line retailers) to resolve issues quickly, without LE/OpSec intervention
		Legal/Civil Action	Help individual victims identify the domain name registrant involved in potentially illegal activity to enable further investigation by LE/OpSec
Business Internet Users (e.g., brand holders, brokers, agents)	Business Domain Name Purchase or Sale	Domain Name Brokered Sale	Enable due diligence in connection with purchasing a domain name
		Domain Name Trademark Clearance	Enable identification of domain name registrants to support trademark clearance (risk analysis) when establishing new brands
		Domain Name Acquisition	Facilitate acquisition of a domain name that was previously registered by enabling contact with registrant
		Domain Name Purchase Inquiry	Enable determination of domain name availability and current registrant (if any)
		Domain Name Registration History	Provide domain name registration history to identify past registrants and dates
		Domain Names for Specified Registrant	Enable determination of all domain names registered by a specified entity (e.g., merger/spinoff asset verification)
Internet Researchers	Domain Name Research	Domain Name Registration History	Enables research and statistical analysis about domain name registrations (also needed by Business Internet Users)
		Domain Names for Specified Registrant	Enables research and statistical analysis about domain name registrants (also needed by Business Internet Users)
		Domain Name Registrant Contact	Enables surveys of domain name registrants (also needed by On-Line Service Providers)
Intellectual Property	Legal Actions	Proxy Service Provider	Enables identification of customer of proxy service associated with a domain name being investigated for possible

User	Purpose	Example Use Cases	Rationale for registration data access
Owners (e.g., brand holders, trademark owners, IP owners)		Customer Identification	infringement or IP theft (i.e., reveal)
		Domain Name User Contact	Enables contact with party using a domain name that is being investigated for TM/brand infringement or IP theft
		Combat Fraudulent Use of Registrant Data	Facilitate identification of and response to fraudulent use of legitimate data (e.g., address) belonging to another registrant
Non-LEA Investigators (e.g., Tax Authorities, UDRP Providers, ICANN Compliance)	Regulatory and Contractual Enforcement	Online Tax Investigation	Facilitate by national, state, province or local tax authority identification of domain name engaged in on-line sales
		UDRP Proceedings	Let UDRP Providers confirm the correct respondent for a domain name, perform compliance checks, determine legal process requirements and protect against cyberflight
		RAA Contractual Compliance	Let ICANN Contractual Compliance audit and respond to complaints about registrar conduct (e.g., data inaccuracy or unavailability, UDRP decision implementation, transfer complaints, data escrow and retention)
LEA/OpSec Investigators (e.g., law enforcement agencies, incident response teams)	Abuse Mitigation	Investigate Abusive Domain Name	Enable effective investigation and evidence gathering by LEA/OpSec personnel responding to an alleged maliciously-registered domain name
		Abuse Contact for Compromised Domain Name	Assist in remediation of compromised domain names by helping LEA/OpSec personnel contact the registrant or designated abuse handler/ISP
Miscreants (e.g., those engaged in spam, DDoS, phishing, identity theft, domain hijack)	Malicious Internet Activities	Domain Name Hijack	Harvest domain name registration data to gain unlawful access to registrant's account and hijacking that registrant's domain name(s)
		Malicious Domain Name Registration	Use an existing/compromised domain name registration account to register new names to support criminal, fraudulent or abusive activities
		Registration Data Mining for Spam/Scams	Harvest domain name registrant data for malicious use by spammers, scammers and other criminals (miscreants)

Table 1. Users

Figure 2 sets forth a non-exhaustive summary of users of the existing WHOIS system, including both those with constructive and malicious purposes. Consistent with the EWG's mandate, all of these users were examined to identify existing and possible future workflows and the stakeholders and data involved in them.

Figure 2: Users

In this report, the term "requestor" is used to refer generically to any of these users that wish to obtain gTLD registration data from the system. As further detailed in Section IV below, the EWG recommends abandoning today's WHOIS model (and protocol) that gives every user the same anonymous public access to (too often inaccurate) gTLD registration data. Instead, the EWG recommends a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.

3.3 Identifying the Purposes to be Accommodated or Prohibited

The EWG sought to prioritize the purposes enumerated in section 3.2 in order to focus use case development and narrow the spectrum of permissible purposes. However, it was difficult to establish a rationale for accommodating the needs of some users that access the current WHOIS system today but not others, so long as their purposes were not malicious. This finding led the EWG to recommend that all of the purposes identified in Section 3.2 be accommodated by the RDS in some manner, with the exception of known-malicious Internet activities that should be actively deterred. The EWG's recommended permissible purposes are therefore summarized below.

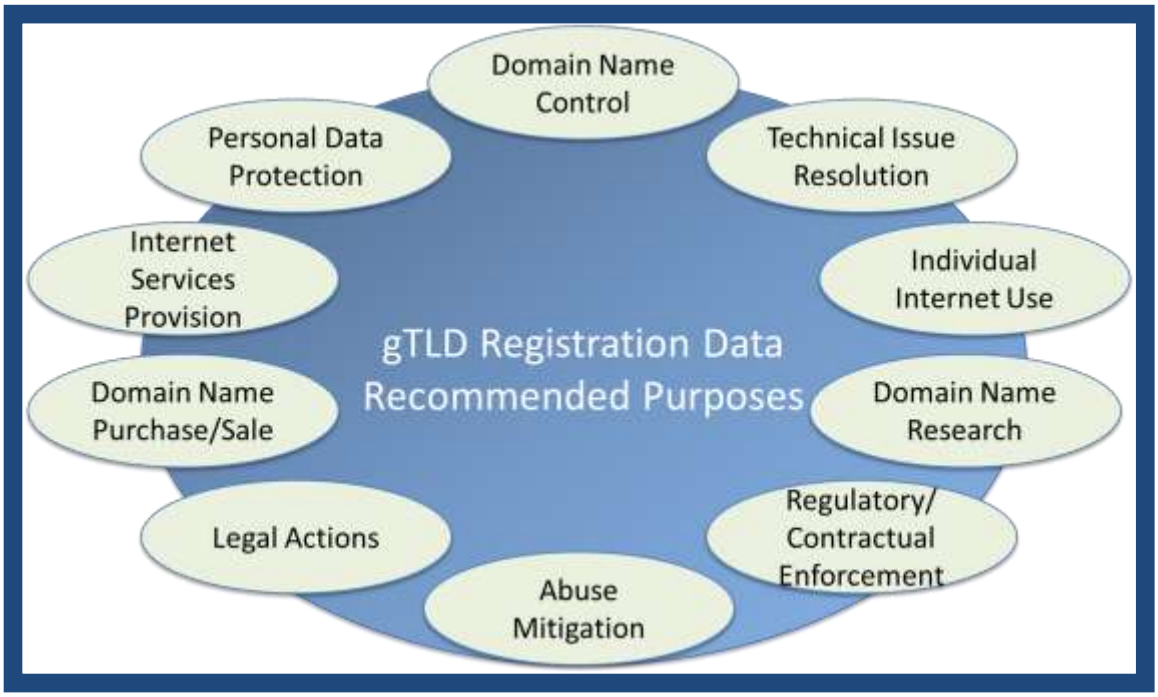


Figure 3: Purposes

It should be noted that, within each purpose, there are an infinite number of existing and possible future use cases. Although the EWG did not attempt to identify all possible use cases, it endeavored to explore a representative sample in hopes of rigorously identifying kinds of users and their purposes in wanting access to gTLD registration data. However, the RDS should be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time.

3.4 Stakeholders Involved in the RDS

The following table provides a representative summary of the various stakeholders involved in collecting, storing, disclosing and using gTLD registration data, mapped to associated purposes. Some stakeholders supply data (e.g., registrants), while others collect/store data (e.g., registrars, registries) or disclose data (e.g., RDS operator, Privacy/Proxy Service Providers). However, most stakeholders are parties involved in initiating data requests (e.g., brand owners, their agents) or parties identified, contacted or otherwise impacted by data disclosed (e.g., domain name abuse contacts). This summary is intended to illustrate the breadth of stakeholders most likely to be affected by the RDS. However, in any given transaction involving registration data, there may well be additional stakeholders not enumerated here.

Stakeholders	Purposes
Abuse Contact for Domain Name	Abuse Mitigation
Acquiring Company	Business Domain Name Purchase or Sale
Acquiring Company's Agents/Attorneys	Business Domain Name Purchase or Sale
Address Validation Service	Domain Name Control
Agents of Registrant	Domain Name Control
Brand Holder	Regulatory/Contractual Enforcement
Brand Management Service Provider	Domain Name Control
Brand Owner	Business Domain Name Purchase or Sale
Certification Authority	Internet Services Provision
Complainant	Regulatory/Contractual Enforcement
Consumers using Websites	Individual Internet Use
Domain Broker	Business Domain Name Purchase or Sale
Domain Buyer	Business Domain Name Purchase or Sale
Fraud Victim	Legal Actions
Fraud Victim's Agent	Legal Actions
Government Agency Personnel	Regulatory/Contractual Enforcement
ICANN Compliance	Regulatory/Contractual Enforcement
Internet Service Providers	Abuse Mitigation
Investigator	Individual Internet Use
Law Enforcement Personnel	Abuse Mitigation Legal Actions
Listed Contacts	Internet Services Provision
Online Service Provider	Internet Services Provision
Op/Sec Service Providers	Abuse Mitigation
Organization Sponsoring Study	Domain Name Research
Person/Entity under investigation	Regulatory/Contractual Enforcement
Privacy/Proxy Service Customer	Business Domain Name Purchase or Sale Domain Name Control Internet Services Provision Regulatory/Contractual Enforcement Personal Data Protection
Privacy/Proxy Service Provider	Abuse Mitigation Business Domain Name Purchase or Sale Domain Name Control Domain Name Research Internet Services Provision Legal Actions Personal Data Protection Regulatory/Contractual Enforcement Technical Issue Resolution
RDS Operator	All Purposes
Registrant	All Purposes
Registrant's Agent	Business Domain Name Purchase or Sale Internet Services Provision Regulatory/Contractual Enforcement
Registrar	Business Domain Name Purchase or Sale Domain Name Control Domain Name Research Individual Internet Use Internet Services Provision Legal Actions Personal Data Protection

	Regulatory/Contractual Enforcement Technical Issue Resolution Abuse Mitigation
Registry	All Purposes
Reporter of Problem	Technical Issue Resolution
Researcher	Domain Name Research
Reseller	Abuse Mitigation
Resolver of Problem	Technical Issue Resolution
Target of Legal/Civil Action	Individual Internet Use
Technical Contact	Technical Issue Resolution
Third Parties seeking Contact	Legal Actions Personal Data Protection
Trusted Agent	Personal Data Protection
UDRP Panelists	Regulatory/Contractual Enforcement
UDRP Provider	Regulatory/Contractual Enforcement
Validator of Heightened Need for Protection	Personal Data Protection
Victim of Abuse	Abuse Mitigation
Web Hosting Provider	Technical Issue Resolution

Table 2. Representative Summary of Stakeholders

3.5 Areas of Commonality

As the EWG analyzed use cases, it became clear that many users have needs for similar data elements, but to satisfy different purposes. Some of these needs are well understood, for example:

- The ability to determine whether a domain name is registered
- The ability to determine the current status of a domain

However, some needs are common and yet not readily fulfilled by the current WHOIS system in a consistent manner. Examples include:

- The ability to determine all domains registered by a given entity
- The ability to determine when a domain was first registered

The EWG took these common needs into consideration when developing recommended principles to guide the design of the RDS. However, since it is likely that further common needs will be identified over time, the system should be designed with extensibility in mind.

3.6 Matching Data Elements to Acceptable Purposes

Annex C *[of the EWG's Initial Report]* describes data elements that are relevant to each acceptable purpose. Ultimately, some of these data elements should be collected for every domain name, while others may be optionally collected for a subset of domain names. Furthermore, collected data elements may or may not be made accessible to requestors through the RDS. The EWG expects to further consider these issues to derive initial recommendations in this area, but recommends that a more thorough risk and impact analysis be performed on each data element to complete this categorization. Public comment would be helpful in identifying how this risk and impact analysis should be conducted, who should conduct it, and the criteria by each data element should be identified as mandatory or optional, for collection and disclosed via public or gated access methods.

IV. DESIRED FEATURES & DESIGN PRINCIPLES

Subject to future appropriate risk and impact analysis in many areas, the EWG believes that the next generation Registration Directory Service (RDS) should incorporate the following features and design principles:

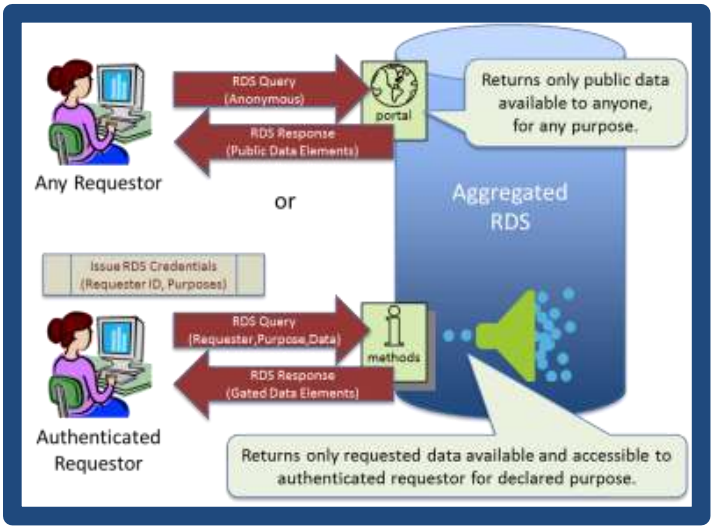
4.5	**Permissible Purposes**	
	4.5.1	• There should be clearly defined permissible/impermissible uses of the system.
	4.5.2	• Section 3 broadly describes the acceptable uses identified by the EWG.
4.6	**Data Disclosure**	
	4.6.1	• The RDS should accommodate purpose-driven disclosure of data elements.
	4.6.2	• Not all data collected is to be public; disclosure options should depend upon Requestor and Purpose.
	4.6.3	• Public access to an identified minimum data set should be made available, with restrictions to limit bulk harvesting.
	4.6.4	• Data Elements determined to be more sensitive after conducting the risk & impact assessment should be protected by gated access, based upon: ○ Identification of a permissible purpose ○ Truthful disclosure of requestor/purpose ○ Auditing/Compliance to ensure that gated access is not abused
	4.6.5	• Some data elements determined (after conducting the risk & impact analysis) to be extremely sensitive could be accessed through defined legal process (e.g., subpoena).
	4.6.6	• Only the data elements permissible for the declared purpose should be disclosed.
	4.6.7	• Annex C *[of the EWG's Initial Report]* describes the data elements identified as relevant to the specific acceptable uses identified in Annex B**.**
4.8	**Access Methods**	
	4.8.1	• Access should be non-discriminatory (i.e., the process should create a level playing field for all requestors, within the same purpose).
	4.8.2	• To deter misuse and promote accountability, ○ All access should be authenticated to the appropriate level; and ○ Requestors needing access to data elements should be able to apply for and receive credentials for use in future authenticated data access queries.
	4.8.3	• Some type of accreditation should be applied to requestors of gated access ○ When accredited Requestors query data, their purpose should be [a] implied, or [b] stated every time a request is made. [*The EWG is expects to explore alternatives a and b further.*] ○ Different terms and conditions may be applied to different purposes. ○ If accredited requestors violate terms and conditions, penalties should apply.

	4.8.4	• All queries/responses should protect the confidentiality and integrity of data in transit.
	4.8.5	• Premium data access services (e.g., Reverse WHOIS, WhoWas) may be offered, subject to some type of accreditation regime.
	4.8.6	• All disclosures should occur through defined access methods. The entire data set should not be exported in bulk form for uncontrolled access.
	4.8.7	• Disclosure may include display and other output methods. ○ To make data easier to find and access in a consistent manner, a central point of access (e.g., web portal) should be offered. ○ Access to public data should be available to all requestors through an anonymous query method (at minimum, via website). ○ Gated access to sensitive data should be supported through web and other access methods and formats (e.g., xml responses, SMS, email), based on requestor and purpose. ○ Requestors should be able to obtain authoritative data in real-time when needed.

VII. ILLUSTRATION OF GATED ACCESS FEATURES

The proposed model for Gated Access (illustrated below) can be summarized as follows:

- A carefully selected subset of data elements would be made publically accessible to anonymous requestors through a web interface to the RDS.
- All other data elements would be made accessible to authenticated requestors only through multi-modal gated access methods supported by the RDS.
- Gated access would only be available to requestors who applied for and were issued credentials to be used for RDS query authentication. The process by which credentials would be issued is not defined herein, but the EWG recommends that this process take into consideration each requestor's purpose for wanting access to registration data.
- Each gated access query would identify the authenticated requestor's purpose (either explicitly or implicitly) and a desired list of data elements. Only data elements that were available for the domain name and accessible to the requestor for the declared purpose would be returned.


RDS Query
(Anonymous)
RDS Response
(Public Data Elements)
portal
Returns only public data available to anyone, for any purpose.
Any Requestor
or
Aggregated RDS
Issue RDS Credentials
(Requester ID, Purposes)
RDS Query
(Requester,Purpose,Data)
RDS Response
(Gated Data Elements)
methods
Authenticated Requestor
Returns only requested data available and accessible to authenticated requestor for declared purpose.

From the EWG's Status Update Report:

a. Improving Accountability

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

As stated in its Initial Report, the EWG believes that a gated access paradigm could increase accountability for all parties involved in the disclosure and use of gTLD domain name registration data. First, the RDS would log all access to gTLD registration data, including anonymous access to public data elements, with restrictions to deter bulk harvesting. In addition, gated access to more sensitive data elements would only be available to requestors who applied for and were issued credentials for RDS query authentication. Finally, the RDS would audit both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use. Different terms and conditions might be applied to different purposes. If requestors violate terms and conditions, penalties would apply.

Proposed User Accreditation for access to Gated Data

The EWG consulted with Europol, Interpol, and other members of the global Law Enforcement community to assess possible accreditation models and bodies. As part of this consultation, the EWG developed a deeper understanding of WHOIS data currently used in criminal and civil investigations, and intends to map this feedback to use cases where data needs differ.

In addition, the EWG has recommended that, for each RDS User desiring access to gated data for permissible purposes, experts should be consulted to identify possible accreditation bodies. As part of this consultation, the EWG expects to review use cases to confirm and better identify what data is needed for various purposes (e.g., brand owners and agents, or Op Sec personnel investigating problems or abuses).

Following further investigation with subject matter experts and public comments about RDS user accreditation for access to gated data, the EWG has drafted the following additional principles, now under discussion:

No.	Additional Gated Access Principles
1.	There should be a non-accredited, anonymous, access method to non-gated data in real-time.
2.	The RDS should only apply the minimum "accreditation scheme" necessary to provide access for the stated purpose.[1]
3.	There should be no need to "pre-approve" or provide credentials to every potential user of the RDS. A request and fulfilment process can be created for each "type" of accreditation.

[1] For example, this accreditation does not need to require multi-factor, sworn statements, or need to be-all-and-end-all system to get most types of data.

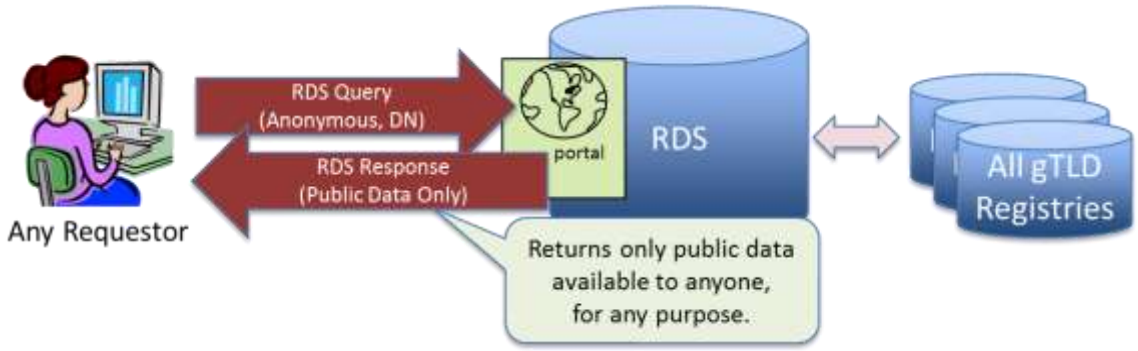
4.	Accreditation for access to data could be granted in four ways/players: • None (anonymous access as above) • Self-accreditation by the person/entity requesting the data (system where the user simply states who they are, perhaps via a standing "account" and what they are requesting and why, and then are granted access to that level of data gives you) – standing account could be used for this. • Accreditation by the subject of the data via a request process (e.g. the person looking up domain requests access for a given purpose, and the subject of that data request grants it) • Some trusted third party
5.	Whenever possible, any third-party RDS accreditation process should leverage existing accreditation processes within a user community identified as one that would need credentialing.
6.	These third-party accreditation processes should be vetted by some authority TBD (for example, ICANN, RDS, panel, etc.) and reviewed on a periodic basis.
7.	Any organization administering them should have a signed agreement with ICANN and/or the RDS to operate such accreditation processes under agreed-upon guidelines and a framework to allow for due process, accountability, security, fair access, and adherence to applicable law.
8.	An organization could apply for accreditation and have all people using the RDS in their organization covered by that one accreditation.[2]
9.	The RDS should be flexible enough to allow creation of both organization-wide and individual credentials for non-anonymous access.
10.	Supplying accreditation for access of RDS data does not have to happen in real-time for all use cases and/or requesters.[3]
11.	The RDS should accommodate automation for large-scale lookups for various use cases and purposes.[4]
12	A single requestor playing different roles may have multiple credentials in order to access different types of data. Within a single role, only one credential should be possible.
13.	Audits and data analytics should be used to identify abuse of the system and access credentials.

[2] It is up to the organization to ensure the integrity of any issued credentials for accessing the RDS.
[3] This allows for both a “registrant approval” or verification process to kick off based on the location of the requestor.
[4] For example, registration data on domains detected hosting malicious content are routinely pulled in via automated processes. This will in-turn populate investigatory tools, kick-off notification processes, and/or provide input into other lookups that attempt to identify malicious infrastructure.

Illustration of Public Data Access

As depicted in the following figure, public data elements can still be requested anonymously via the RDS. Refer to **Annex A** *[of the EWG's Update Report]* for more detailed illustration of data elements returned to an anonymous public data query.

Anonymous Public Registration Data Access via RDS



Annex A *[of the EWG's Update Report]* also contains an example use case to illustrate the steps involved in accessing the relevant data elements.

As depicted in the following figure, gated data elements can also be requested via the RDS. To do so, requestors must first be accredited. Thereafter, requestors may submit authenticated queries requesting data elements for a stated purpose. Refer **Annex A** *[of the EWG's Update Report]* for more detailed illustration of data elements returned to an authenticated gated data query.

Gated Registration Data Access via RDS