

**Accreditation & Access Model
For Non-Public Whois Data
March 23, 2018
Version 1.2**

Introduction

To the ICANN Community:

On May 25, 2018, the General Data Protection Regulation (GDPR) will come into effect. In advance of that date, the domain name community has been working together to ensure systems are prepared and policies are in place.

However, important functionalities of the WHOIS system remain unaddressed. ICANN's proposed model has not addressed the public interest -- specifically, we have not ensured an access to WHOIS data for law enforcement, cyber security and consumer protection interests. This oversight leaves Internet users unprotected.

Many are concerned. The Governmental Advisory Committee forcefully advised the ICANN Board in its [ICANN 61 communique](#) to maintain WHOIS to the fullest extent possible and mandate an access mechanism. This view is also held by the Commercial Stakeholders Group and the At Large Advisory Committee.

Accordingly, during the ICANN 61 meeting in San Juan, Puerto Rico, the Business and Intellectual Property Constituencies proposed, and the community discussed, a credible model to ensure continued WHOIS availability for eligible entities seeking data access. Based on feedback from many, including contracted parties, the model was further refined and is found herein.

Time is of the essence. Should an accreditation and access model not be agreed upon in the next few weeks, the danger is that WHOIS effectively will "go dark" on May 25. Such a development would disable a critical tool employed for the safe, stable operation of the DNS, the prevention of crime, the conduct of vital cybersecurity operations, the protection of consumers, and the enforcement of intellectual property rights. By ICANN's own estimation, an outage of that kind could last until December 2018, or longer.

To prevent such a development, this model seeks to provide access to law enforcement, cyber security interests, intellectual property owners and others charged with protecting Internet users. We now seek the further collaboration of contracted parties and the ICANN org in order to avoid such perils and swiftly move this model toward a workable implementation. And while this model is proposed for generic top-level domains, we encourage consideration by country code TLDs as well. We encourage your input and suggestions, and thank you for your consideration.

**Accreditation & Access Model
For Non-Public Whois Data
March 23, 2018
Version 1.2**

Preface & Overview

This document provides a framework for the rapid implementation of a certification and access model for non-public WHOIS data for legitimate and lawful purposes¹.

Compliance with GDPR will severely restrict public access to WHOIS data elements -- elements that are critical to multiple functions within the DNS. Such a restriction will undoubtedly impact the ability of law enforcement and those involved with consumer protection to investigate wrongdoing; this is a significant development, considering:

- Bad actors operate at scale, across multiple top-level domains, sometimes using thousands of names in coordinated and automated attacks.
- Harms range from consumer fraud, spam, phishing, botnet attacks, and distributed denial of service attacks to the more grim, including human trafficking and child abuse.
- The harm inflicted is often dangerous, painful, irreversible and swift, and carries consequences that are problematic for Internet users.

WHOIS data elements are extraordinarily useful in preventing or in investigating and prosecuting against these harms. For example:

- within WHOIS, a point-of-contact data element, or elements in combination, are often used to expand an investigation beyond a single abused domain to a larger set, potentially used to scale harms exponentially.
- attribution is critical to minimizing false positives when attempting to discriminate between maliciously and legitimately registered domain names and host names
- automated access for a specific legitimate purpose enables surgical, proactive security blocking to prevent spam, phishing attacks, and other abuse from reaching consumers.

This model, accordingly, presents an available solution to the problem of access to non-public data elements. Documented here are:

- the types of eligible entities that may seek access to data;
- legitimate and lawful purposes for accessing data;
- how eligible entities may be accredited to access data;
- a proposed operating model and
- terms of accreditation.

¹ Much like the “tiered access” model proposed in the Expert Working Group’s *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*, p. 86, <https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf>

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

Note that this model specifically excludes law enforcement agencies (LEA) and other governmental access, though such access could be provided and validated in a similar fashion.

Under this model, defined groups of organisations or categories of organisations can gain access to gated data if they (1) require access to data for specific, legitimate and lawful purposes, and (2) are properly validated by a third-party accreditor.

This descriptive document is intended as the basis for creation of a functional specification for implementation. (For a similar approach, see the TMCH Functional Spec Example²)

Eligible Entities & Eligibility Requirements

Eligible entities highlighted here for this purpose are derived from the entities and use cases documented in the Expert Working Group's final report on gTLD Directory Services.³ As such, the three Eligible Entities discussed here do not represent the finite universe of all possible Eligible Entities, but include those having legitimate and lawful purposes to access data, as well as agents that facilitate protection of public interests, security and lawful behavior alongside Eligible Entities.

1. Cybersecurity & OpSec Investigators

Eligible Entities would include individuals and companies who provide cybersecurity or operational security for themselves, a corporation, or provide it as a solution and/or service to other individuals or entities. Examples of such services include:

- security intelligence and analytics;
- identity and access management;
- application security;
- fraud protection;
- digital forensics and incident response;
- email and data security; and
- protection from spear-phishing and malware, botnets, DDOS attacks.

The application template for applicants in this category includes:

- Identity of the applicant
- Contact information
- Standing for application (organizational mission)
- Evidence of organizational formation or incorporation
- Statement regarding intended use of data

² <https://tools.ietf.org/html/draft-lozano-tmch-func-spec-10>

³ Id. At 21, table of use cases in EWG report

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

To aid in accreditation, entities may also:

1. provide:
 - a. Verifiable credentials; and
 - b. letters of authority/endorsement from governments, companies, and/or individuals on whose behalf they are authorized to act (e.g., hired to protect from security threats including but not limited to spam, malware, malicious apps, denial of service, ex-filtration of content, persistent threats, fraud and other harms).

And must also:

2. be willing to agree to:
 - a. the terms of service,
 - b. prevent abuse of data accessed,
 - c. be subject to de-accreditation if they are found to abuse use of data, and
 - d. be subject to penalties

Examples include: Akamai, BAE Systems, Cloudflare, IBM Security, Sophos, Symantec.

2. Intellectual Property

This category is designed for intellectual property rights holders, including trademark, patent or copyright owners or their attorneys or agents (agents may include legal representatives, trade associations, data aggregators and brand protection companies). Applicants in this category may also include members in good standing of a national or state/provincial licensing organization (such as a bar association, or a patent and trademark office), or of a related trade association (such as the International Trademark Association). Applicants must provide:

- evidence of ownership of intellectual property rights (e.g., a trademark registration); or
- letters of authorization from the rights holders to act on their behalf; or
- Proof of membership in good standing

This category of user must also:

1. Agree to use the data for legitimate and lawful purposes
2. Further agree to:
 - a. the terms of service;
 - b. prevent abuse of data accessed; and
 - c. be subject to de-accreditation if they are found to abuse use of data.

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

3. Non-governmental Public Safety and Health Organizations

Eligible entities include not-for-profit organizations that seek to protect public safety and health. Their legitimate and legal purposes include:

- Academic and other non-profits with a legitimate or legal purpose
- Child protection and child anti-abuse organizations
- Combating human trafficking
- Combating counterfeit pharmaceuticals
- Combating dangerous counterfeit products
- Combating hate, racism and discrimination

The application template for applicants in this category includes:

- Identity of the applicant
- Contact information
- Standing for application (organizational mission)
- Evidence of organizational formation or incorporation
- Statement regarding intended use of data

This category of user must also:

1. Agree to use the data for legitimate and lawful purposes
2. Further agree to:
 - a. the terms of service,
 - b. prevent abuse of data accessed,
 - c. be subject to de-accreditation if they are found to abuse use of data, and
 - d. be subject to penalties

Examples include The Internet Watch Foundation, NCMEC, LegitScript, The Southern Poverty Law Center, the Anti-defamation League.

Vetting and Accreditation

Users are to be vetted by accreditation authority, based on credentials presented. Contracted parties are not expected to perform further vetting.

Validation and Review of Access Purposes

Accreditations for Eligible Entities will be subject to periodic review by the accrediting authority to ensure they meet the access purpose criteria set forth by that authority. Appeal mechanisms will apply in the instance that a review results in de-accreditation.

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

Legitimate and Lawful Purposes

This section contains a list of legitimate and lawful purposes for the above accredited Eligible Entities. Each purpose is mapped to an entity type.

Legal Actions

- Investigate fraudulent use of registrant's name by any other domain names
- Contact a registrant's legal representative
- Take legal action

Intellectual Property Enforcement

- Investigate possible intellectual property infringement
- Contact infringing parties
- Research a domain name's historical record
- Identify other domains registered with a given name or address
- Initiate or facilitate administrative proceedings

Security / DNS Abuse Mitigation

- Track and predict malicious behavior
- Investigate security and abuse trends
- Contact victims with compromised domain names
- Enable domain name white/black list analysis by security/reputation service providers

Regulatory and Contractual Enforcement

- Contractual compliance investigation
- Registration data escrow audits

Domain Name Administration

- Transfers of a domain between registrars or registrants

Public Health and Safety

- Gather evidence of activity dangerous to public health or safety
- Identify other domains registered with a given name or address that may be involved in activity that threatens public health or safety
- Report to government agency or law enforcement

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

Purpose and Entity Mapping⁴

Purpose	Entity - Reason
Legal Actions	<ul style="list-style-type: none">• Security - To investigate/remediate fraud• IP - To investigate/remediate infringement
Intellectual Property Enforcement	<ul style="list-style-type: none">• IP - To investigate/remediate infringement, fraud, cybercrime
Security / DNS Abuse Mitigation	<ul style="list-style-type: none">• Security/IP - To investigate/remediate and block criminal activity, fraud, technical exploits
Applicable Law, Regulatory and Contractual Enforcement	<ul style="list-style-type: none">• Private Sector IP and Security - for investigation of crimes and DNS abuse for the purpose of protecting users from fraud and assembling data for Law Enforcement Agency response
Domain Name Administration	<ul style="list-style-type: none">• IP - To administer domains• Others - Contracted party usage not in scope, but they and others may need access to ensure chain of custody/ownership of domains for transfers and transactions.

Certification Process⁵

All Eligible Entities must:

- 1) Submit an application with verifiable
→ contact details
 1. Name
 2. If Applicant is an agent, the name of individual or entity for whom agency exists
 3. Physical Address
 4. E-mail Address
 5. Telephone number
- 2) and required documentation

⁴ See also EWG report p.21

⁵ Note additional scenarios for accreditation in Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 63,

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

- Cybersecurity & OpSec Investigators: Verifiable credentials and letters of authority
 - Intellectual Property: Evidence of IP ownership or a letter of authorization from the rights holder to act on its behalf
- 3) undergo validation by an ICANN approved agent (like the services offered by certificate authorities or those offered by Deloitte for the trademark clearinghouse)

Once the Eligible Entity successfully completes steps 1 and 2 above, the ICANN approved agent issues one of two decisions:

- The applicant is issued user credentials or a certificate.
- Or
- Rejection of the application

Eligible entities will be presumed to be qualified for accreditation. However, accreditation can be denied for various reasons, including documentation that is out of order, previous violations of terms of use, or other reasons.

*Any Eligible Entity that receives login credentials must go through annual reaccreditation.

Proposed Operating Model

The new models conceived and considered in the *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)* are not workable due to the distributed nature of Whois databases. Under those models, each contracted (registry or registrar) party operating a Whois database will need to govern access. No changes are proposed to the existing Whois infrastructure other than creating gated access for individual record or automated access of Whois records including non-public elements. Collection, storage, and copy models are unaltered; however, authorization and access⁶ changes are necessary.

In this proposed model, which is a federated model for access to Whois, eligible accredited entities can present their credentials to any Whois system. Contracted parties collect credentials, which are validated by a central authority, and the requesting entity is either granted or denied access to data.

Accredited Users

Upon accreditation, users are given credentials to access Whois data. . Users are able to present their credentials to a Whois database operator who validates credentials with a federated, centralized access authority and then provide access to Whois data. Responses to

⁶ Note Models Considered, Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 110

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

single record queries should be delivered via browsers and automated access should be delivered via port 43 .

Contracted Parties and Agents

Within one business day of being presented with them, Contracted Parties (registries and registrars) and agents will accept credentials and provide access to non-public data for accredited users. They will rely on a centralized access authority to validate user credentials and then provide or deny access. Users will then be able to issue single-record or bulk queries against the Whois databases. Once presented with credentials from the accreditation authority, contracted parties cannot unreasonably withhold access to data.

Logging

All accredited entities and agents query activity will be logged. Logs will include accredited entity, purpose, query, and date,. Logs must be retained in a machine readable format. Logs must be kept up-to-date with each new query. In the event of an audit or claim of misuse, logs may be requested for examination by an accreditation service or dispute resolution provider. Logged data must substantiate that accredited users are using data for legitimate and legal purposes as detailed above. Each query must be mapped to a purpose that is applicable.

Abuse Reporting

The system will be suitably transparent to allow third party examination of query rate and volume. A mechanism will be provided for reporting over-extensive use, mirroring or other abuses to the accreditation authority, who will retain the right to investigate and, if necessary, revoke accreditation. The accreditation authority also may refer the offending party to Data Protection Authorities.

Audit

A third-party firm should randomly audit a small sample of query logs for compliance with terms and conditions funded by accreditation and renewal fees. Additionally, Whois database operators may, once annually and at their expense, demand an audit of any accredited entity. A Whois database operator's logs for access may be matched to an accredited entity's logs by a third-party to discern misuse/abuse. (see EWG report Accountability and Audit Principles⁷) Also, query logs should cite purposes of access, which must be tied to a legitimate and legal use case for each accredited users use case. Audits will be conducted by a third-party bonded company, and logs are to be delivered with identity of the log origin tokenized or anonymized so that the auditing organization cannot see and thus risk identifying methods of accredited party.

⁷ Note Audit Principles, Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 94,

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

Accreditation Renewal

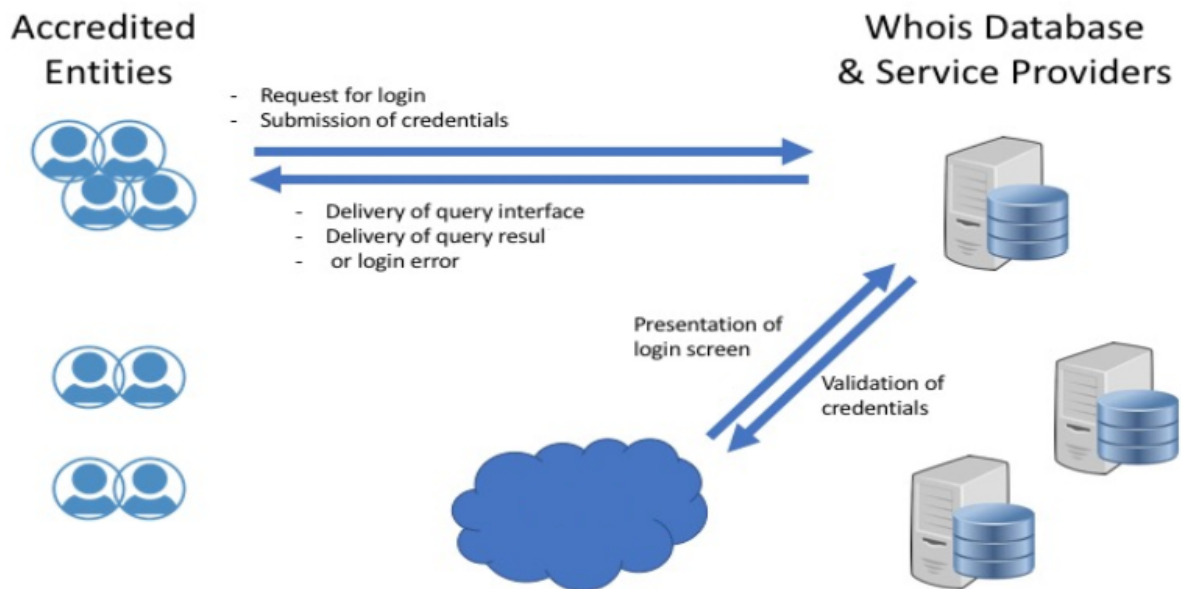
Accredited parties must renew their accreditations annually. Renewals must incorporate updated terms of service or other obligations imposed by the accreditation authority. User fees are due and payable upon the date of renewal, with further access conditioned upon successful payment. Then current certification documentation must be provided. Accreditation authority reserves the right to change the credentials or other material required for accreditation.

Central Access Authority

Login and authorization for access by accredited entities to Whois database operators at registries and registrars will be provided by a third-party or parties

Application and renewal fees should be sufficient to cover onboarding and support fees for the authorization and access system. Application and renewal fees should scale with the number of users for each accredited entity. Contracted Parties and Agents should need minimal support to integrate this authorization system into their workflow for gated access. Support for integration at contracted parties should come at no cost and be fee-based for agents.

Federated Access for Whois Diagram



Complaints

- Complaints regarding accuracy of data will be addressed directly to the domain name's sponsoring registrar for resolution.

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

- Complaints regarding performance of underlying WHOIS providers will be directed to ICANN compliance, who will address the matter with the appropriate registrar, according to the terms of the Registrar Accreditation Agreement.
- All other available remedies (e.g., filing false WHOIS complaints) are available to all appropriate parties.
- Complaints regarding unauthorized access to or improper use of data will be addressed to the accrediting agency, who will have the authority to restrict or deny further access to WHOIS data.

Penalties

The accrediting agency will audit both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor.

Different terms and conditions could be applied to different purposes. Violation of terms and conditions may result in graduating penalties, including but not limited to:

- Restricted or throttled access
- Denial of further access
- Financial penalties

Terms of Accreditation

Data Protection

Accredited users must protect the personal data in their custody queried from Whois systems and adhere to applicable law for the handling of personal data. At a minimum, individual companies and users have a responsibility to protect data at rest by accessing it on machines that are protected by passwords and have adequate security facility. Similarly, agents have a responsibility to protect the data that they provide to others, and therefore must:

- 1) gate access to data via password
- 2) secure data at rest through encryption
- 3) secure data in transit through encryption
- 4) validate with each login that users have up-to-date accreditation for use of the data.

Application Fees

All applicants must pay a non-refundable application fee proportional to the cost of validating an application. Rejected applicants may re-apply up to two times, each time paying the fee. Fees are to be established by validation authority.

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

Data Access

Accredited data access is to be provided for legitimate uses either for single record queries or automated queries for analysis. Accredited access shall not be rate-limited or otherwise restricted except as needed to ensure operations; any accredited user may have access to all Whois records from any ICANN contracted party. Data may be stored by accredited users for analysis and collection of case data. Stored data must at a minimum be secured by password and encryption, and use of and access to data must conform with terms of service. As stated above, accredited users and organizations must protect the personal data in their custody queried from Whois systems and adhere to applicable law for the handling of personal data.

Data Misuse Penalties

In the event of breach of the terms and conditions, any legitimate user's right to access, retain or use data is suspended. Upon being notified of a breach, a user's access privileges are revoked and that user must delete any retained data and provide notice to the certifying body that the data has been deleted. Data misuse violations may be appealed to accrediting body (see EWG report, RDS User Accreditation Principles⁸) and access may be reinstated at the discretion of that body.

Agents that provide data to other accredited users are responsible for denying access to formerly accredited users whose privileges have been revoked for their misuse. Agents are also responsible for validating that their users are accredited and maintain accreditation; they must provide access only to currently accredited users or they are subject to misuse penalties.

Data Misuse

Data is not to be misused in any manner by any party. Categories of misuse could include the following non-exhaustive examples:

- Non-legitimate purposes (e.g., registration data mining for spam/scams)
- Data revealed as a result of a security breach
- Provision or sale of data to non-accredited parties for any reason
- Use of data for a purpose that is inappropriate for the accredited user type.

⁸ Note RDS User Accreditation Principles, Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 62

ANNEX A: PURPOSE STATEMENT FOR THE COLLECTION AND PROCESSING OF WHOIS DATA

The GDPR requires that the collection and processing of personal data be for “specified, explicit and legitimate purposes.” (Article 5(1)(b). In addition to processing that is necessary for the performance of a contract to which the data subject—in this case a registrant—is party, the GDPR permits processing that is necessary for the public interest or the legitimate interests pursued by a third party. (Article 6)

The following purpose statement meets the requirements of the GDPR, keeps in line with the proposals of the EWG’s final report⁹ and ICANN’s Cookbook,¹⁰ and supports the public interest and expectation by individual users that the Internet be a safe and secure place by ensuring safety and security through accountability.

The Internet is a public resource governed by a set of private arrangements that replace a system that otherwise would be created by national and international laws. These private contracts, executed under the oversight of ICANN, come with responsibilities, to serve many public policy interests -- especially because (as seen in ICANN bylaws) ICANN’s mandates go beyond the mere technical function of mapping names to numbers.

One of these contractual obligations is WHOIS. The WHOIS system plays a key role in accountability online and ICANN needs to adapt the current WHOIS system to comply with the GDPR in line with its [new Bylaw](#) commitments requiring that ICANN "use commercially reasonable efforts to enforce its policies relating to registration directory services and work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."

As such, in support of ICANN’s mission to coordinate and ensure the stable and secure operation of the Internet’s unique identifiers, personal data included in domain name registration data may be collected and processed for the following purposes:

⁹ Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 16,

<https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf>

¹⁰ The Cookbook, Section 7.2.1, At 34.

<https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf>

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

1. Providing access to accurate, reliable, and uniform registration data in connection with the legitimate interests of the registrar and WHOIS system stakeholders;¹¹
2. Enabling a dependable mechanism for identifying *and* contacting the registrant;
3. Enabling the publication of points of contact administering a domain name;
4. Providing reasonably accurate and up-to-date information about the points of contact administering a domain name;
5. Providing access to registrant, administrative, or technical contacts for a domain name to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection;
6. Providing registrant, administrative, or technical contacts for a domain name to address appropriate law enforcement needs;
7. Facilitating the provision of zone files of gTLDs to Internet users;
8. Providing mechanisms for safeguarding registrants' registration data in the event of a business or technical failure, or other unavailability of a registrar or registry;
9. Coordinating dispute resolution services for certain disputes concerning domain names; and
10. Ensuring that ICANN fulfills its oversight responsibilities and preserves the stable and secure operation of the Internet's unique identifier systems through at a minimum, addressing contractual compliance functions (including complaints submitted by registries, registrars, registrants, and other Internet users) as well as other necessary oversight functions, such as reporting, policy development, and implementation.

The following chart ties this purpose statement to the performance of the domain name registration contract between the registrar and the registrant, public interests and legitimate interests pursued by a third party:

¹¹ GDPR Art. 6(1)(f)

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

Purpose	Objective	Basis/Interest	Processing	Indicative Users
Domain Name Initial Purchase/ Registration, Management and Control	Tasks within this purpose include creating, managing and monitoring a Registrant's domain name (DN), including creating the DN, updating information about the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and validating the Registrant's contact information (pursuant to RAA requirements).	Performing and satisfying contractual obligations	-Collection of the data; transfer of data to registry and escrow providers to ensure preservation of data -Inter registrar transfers -Validation of Registrant data for accuracy. - Validation for any restricted TLDs -Zone file provisioning -Storage for retention at least during registration term	Registrants, Registrars, Registry Operators, Escrow Providers, privacy proxy providers, ICANN

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

<p>Business/Personal Domain Name Purchase or Sale</p>	<p>Tasks within this purpose include making purchase queries about a DN, transferring a DN to another Registrant, acquiring a DN from another Registrant, and enabling due diligence research by the purchaser to ensure that the DN is suitable for purchase and that the seller is bona fide. To accomplish these tasks, the user needs access to the Registrant's Organization and email address, and in some cases additional data – for example, to perform a Reverse Query on the name of a Registrant or contact to determine other domain names with which they are associated.</p>	<p>Prerequisite for functioning marketplace for DNs</p>	<ul style="list-style-type: none">-Validating Registrant email contacts for transfers-Contacting Registrant for potential sale- Performing reverse query on registrant information to ensure the sale will meet specific business criteria.-Foregoing requires storage, publication and access of WHOIS data	<p>Registrants, potential DN buyers, resale agents, Registrars</p>
---	---	---	---	--

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

<p>Technical Issue Resolution</p>	<p>Tasks within this purpose include working to resolve technical issues associated with DN use, including email delivery issues, DNS resolution failures, and website functional issues. To accomplish these tasks, the user needs the ability to contact technical staff responsible for handling these issues. (Note: It might be useful to designate multiple points of contact to address various kinds of issues – for example, postmaster for email issues.)</p>	<p>Providing security and stability of the DNS, consumer protection, and protection of Registrants expectation of service Providing a pathway for resolving technical problems/ issues</p>	<p>- Validation of Registrant information -Provision of access to technical users. -Foregoing requires storage of access to technical contact information</p>	<p>Registries, Registrars (Network Operations); DNS service providers; cybersecurity experts</p>
<p>Domain Name Certification</p>	<p>Tasks within this purpose include a Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name. Registrants seek certification to increase consumer trust and confidence in their website associated with the DN. To accomplish this task, the user needs to confirm that the DN is registered to the certificate subject; doing so requires access to full WHOIS data</p>	<p>Protecting registrant's interest in maintaining secure DN Providing consumer protection and security</p>	<p>-Validation of registrant contact info for EV, DV, OV SSL certifications -Foregoing requires storage of and access to full WHOIS data</p>	<p>Certificate Authorities, SSL Certification providers, Registrants, Registrars</p>

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

	about the Registrant.			
--	-----------------------	--	--	--

<p>Individual Internet User Protection Security and Trust</p>	<p>Tasks within this purpose include identifying the organization/service provider using a DN to instill consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them. To accomplish these tasks, the user needs the name of the organization/service provider (preferably identity-validated) and its email address, and may benefit from following a contact URL to a page that describes the organization/service provider and its customer service contacts or allows the user to submit a customer service inquiry.</p>	<p>Safety, consumer trust and protection, validation of trustworthiness of the information provider.</p>	<p>-Validation of organization/service provider contact information -Provision of access to consumers and other third parties relying on services/information being provided by the organization/service provider - Foregoing requires storage and publication of and easy access to WHOIS data</p>	<p>Consumers and the general public</p>
---	--	--	---	---

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

<p>Academic/ Public Interest DNS Research</p>	<p>Tasks within this purpose include academic public interest research studies about DN including public information about the Registrant, the domain name's history and status, and DNs registered by a given Registrant (Reverse Query). To accomplish these tasks, the user needs the ability to access all public data in the WHOIS directory and in some cases may need access to data for use in anonymized, aggregated form.</p>	<p>Promotes broad range of research purposes to improve function, use security, and stability of the DNS; Supports freedom of expression and academic research</p>	<p>- Access to public data and certain non-public data in anonymized form. - Foregoing requires the storage, publication and access to WHOIS data</p>	<p>Students, research orgs, journalists, and academics</p>
---	---	--	---	--

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

<p>Legal Actions</p>	<p>Tasks within this purpose include investigating possible fraudulent use of a Registrant's name or address by other registrants, investigating possible trademark infringement, fraud, copyright infringement, or other civil law violations, contacting Registrant or Registrant's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed. To accomplish these tasks, the user needs the ability to contact the Registrant or its legal representative, without relay through an accredited Privacy/Proxy provider.</p>	<p>Investigating and remediating possible IP infringement or other civil law violations</p> <p>-Preventing fraud and other forms of abuse</p> <p>-Facilitating the establishment, exercise, or defense of legal claims</p>	<p>-Disclose to third party IP rights owners; potential legal complainants</p> <p>- Facilitate identification of and response to fraudulent use of legitimate data (e.g., address) for domain names belonging to the same or other Registrant by using Reverse Query on identity-validated data.</p> <p>-Foregoing requires the storage, retention, publication and access to the full WHOIS data; enabling reverse WHOIS lookup</p>	<p>IP lawyers; intellectual property owners, brand protection and enforcement services companies and associations; cybersecurity experts; Registrars; Registry Operators</p>
----------------------	---	--	--	--

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

<p>Regulatory and Contractual Enforcement</p>	<p>Tasks within this purpose include tax authority investigation of businesses with online presence, UDRP or URS investigation, contractual compliance investigation, and registration data escrow audits. To accomplish this, user needs access to Registrant contact and DN data elements, such as email address and telephone number, as appropriate for the stated purpose. For example, WIPO may need access for UDRP resolution.</p>	<p>-Supports audit and enforcement of private and public legal obligations</p> <p>-Supports security, stability and trustworthiness of DNS</p>	<p>-Storing and disclosing data to regulators, ICANN and authorities entrusted with UDRP, URS adjudication.</p> <p>-Foregoing requires storage, retention and access to WHOIS data.</p>	<p>Regulators, ICANN Compliance, Parties to contracts, Administrative and enforcement entities such as WIPO</p>
---	--	--	---	---

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

<p>Public Health and Safety Protection and Criminal Investigation</p>	<p>Tasks within this purpose include investigating and reporting threats to public health and safety, including reporting such threats to third party that can investigate and address that threat/abuse, derive investigative leads, serve legal process and/or contact entities associated with a domain name during a criminal investigation. To accomplish these tasks, the law enforcement agent, first responder, public health and safety organizations (e.g. Internet Watch Foundation) needs to quickly and reliably identify the Registrant and all other entities involved with this service provision / maintenance</p>	<p>Public health, safety and security</p> <p>Investigating cyber- crimes and cyber-enabled crimes;</p>	<p>-Detecting abuse by providing access to Registrant data for protecting public health and safety, including by accessing historic full WHOIS data for some period of time</p> <p>-Providing access to Registrant data for the purposes of detecting and mitigating criminal activity, including by accessing historic full WHOIS data for some period of time</p> <p>-Reporting abuse and potential criminal activity, including sharing WHOIS data among multiple public health and safety organizations, organizational and corporate digital crimes teams, law enforcement agencies in multiple jurisdictions to address cross-border nature of abuse/criminal activity</p> <p>-Foregoing requires storage,</p>	<p>Law enforcement and government or private entities entrusted with enforcement responsibilities; public health and safety organizations, including victim advocacy organizations; digital crime/abuse teams.</p>
---	---	--	--	--

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

			retention and access to full WHOIS data; enabling reverse WHOIS lookup to determine breadth and scope of abuse and properly identify person/entity responsible for abuse and/or criminal activity.	
--	--	--	--	--

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

<p>DNS Abuse Study, Investigation and Mitigation</p>	<p>Tasks within this purpose involve identifying the proliferation of malware, botnets, spam, phishing, identity theft, DN hijacking, data hacking, distributed denial of service attacks (DDOS), etc, and deploying mitigation measures to combat such abuses.</p> <p>Tasks in this purpose also include processes that security professionals use to defend their organizations' networks including risk assessing domains that trip alerts on their network (domains attempting to communicate with the network, or for example employees attempting to navigate to websites), as well as correlating WHOIS data with other network telemetry and contextual data they may have on these domains, pivoting from one domain to map resources controlled by active attackers, and if necessary driving to attribution of these attacks to the individuals and organizations behind them.</p>	<p>Protecting Registrant from abuse and hijacking of Registrant's DN</p> <p>Consumer trust in the Internet</p> <p>Ensuring network and information security and stability of the DNS</p> <p>Combating unlawful or malicious/abusive actions negatively affecting secure and stable functioning of the DNS</p>	<p>-Providing access to Registrant data for the purposes of detecting and mitigating DNS abuse</p> <p>-Foregoing requires storage, retention, publication and access to WHOIS data; enabling reverse WHOIS lookup</p>	<p>Law enforcement and public safety agencies;</p> <p>Cybersecurity firms and individual cybersecurity analysts and experts;</p> <p>Registry Operators, Registrars</p> <p>ICANN Compliance</p>
--	---	---	---	--

Accreditation & Access Model

For Non-Public Whois Data

March 23, 2018

Version 1.2

ICANN DNS Oversight	Tasks within this purpose involve ensuring that ICANN fulfills its oversight responsibilities and preserves the stable and secure operation of the Internet's unique identifier systems, through at a minimum, addressing contractual compliance functions (including complaints submitted by registries, registrars, registrants, and other Internet users) as well as other necessary oversight functions, such as reporting, policy development, and implementation.	-Promoting choice and competition and ensuring the stability, security, and resiliency of the DNS -Addressing contractual compliance obligations -Supporting audit and oversight functions	Storing and disclosing data to ICANN -Foregoing requires storage, retention, publication and access to WHOIS data	ICANN organization
---------------------	---	--	--	--------------------