Draft Accreditation & Access Model
For Non-Public Whois Data
April 20, 2018
Annotated Version 1.4

Introduction

During the ICANN 61 meeting in San Juan, Puerto Rico, the community discussed an accreditation and access model to ensure continued Whois availability for eligible entities seeking data access. Based on feedback from many, including members of the contracted party house (registrars and registries) and security interests (e.g., some SSAC members), the model has been refined. A community-wide discussion of the refined model was held on April 6, where further input was received. All members of the community were invited to the discussion and encouraged to submit written comments and input to the proposed accreditation and access model. Those comments are incorporated into this version (numbered 1.4) -- a descriptive document intended as the basis for creation of a functional specification for implementation. (For a similar approach, see the TMCH Functional Spec Example)

Significant amounts of resources are being devoted to this proposed accreditation and access model through a broad-based effort to avoid the possibility that Whois effectively will "go dark" on May 25. (See **Annex B** for background on why this is critical to the safety and security of the Internet and its users).

We now seek further community input and formal ICANN Org support to execute upon this model, including resources for design and implementation on an accelerated timeline in advance of the May 25 implementation date for GDPR compliance.

Overview

This document provides a framework for the implementation of an accreditation and access model to provide access to non-public Whois data for legitimate and lawful purposes -- much like the "tiered access" model proposed in the Expert Working Group's Final Report (EWG Report).[1]

Building on ICANN Org's proposed model that recognizes a legitimate basis for the continued collection of full thick Whois data by registrars, this accreditation and access model presents an available solution to the problem of access to non-public data elements while respecting the imperative of data privacy and complying with GDPR. Under this model, defined groups of organizations or categories of organizations 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.

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;

[1] Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS) at p. 86

- A proposed operating model; and
- Terms of accreditation.

Note that this model does not include specific provisions for law enforcement agencies (LEAs) and other governmental access, which is extremely important and is being addressed by government representatives separately. To the extent that governments wish to adopt elements of this criteria and adapt them for LEA accreditation, that would be welcomed, as would further collaboration and consultation between government and private sector representatives.

Eligible Entities: Purposes & Eligibility Requirements

The four types of Eligible Entities highlighted here are derived from the list of entities and use cases documented in the EWG Report,[2] and are not an exhaustive list. They include those having legitimate and lawful purposes to access data, as well as agents that facilitate protection of public interests, security and lawful behavior.

1. Cybersecurity & OpSec Investigators[3]

This category is designed for security companies, organizations that need to protect their own interests and agents/companies that act on their behalf. Eligible Entities include companies, or individuals at companies, who provide cybersecurity or operational security for their company or another organization, or provide it as a solution and/or service to other individuals, entities or end-users. Agents may include cybersecurity concerns, financial institutions, academic institutions and researchers, OpSec investigators, and threat intelligence providers who aggregate data for correlation.

Legitimate and lawful purposes for access include:

- Investigating, tracking and preventing malicious behavior
- Researching and investigating security and abuse trends
- Contacting victims with compromised domain names
- Enabling domain name white/black list analysis by relevant service providers
- Maintaining integrity, availability and continuity of online platforms
- Initiating or facilitating legal proceedings

Examples of services covered include:

- Identity and access management
- Application security
- Fraud protection
- Bank and payment processors and their compliance providers

[2] *Id.* at 21, See table of use cases in EWG report

[3] SSAC members are working to create a proposal for appropriate credentialing of cybersecurity interests and are considering models like those used for the Anti-Phishing Working Group (APWG), their APWG Malicious Domain Suspension (AMDoS) model, and other relevant security vetting protocols. Other models that could be used include the Trusted Community Representative (TCR) used for DNSSEC.

- Digital forensics and incident response
- Email and data security
- Protection from spear-phishing and malware, botnets, DDOS attacks
- Protection for end-users by online platforms, such as browsers, search engines, and social media companies
- Security intelligence and analytics
- Ensuring continuity, integrity and availability of Internet infrastructures

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 agree to follow vetting and accreditation processes (see below).

Examples of entities in this category include: ICANN, HSBC, JPCERFT/CC, REN-ISAC, Akamai, BAE Systems, Cloudflare, IBM Security, Sophos, Symantec and security organizations within companies like Salesforce, Facebook, Microsoft.

2. Intellectual Property Abuse[4]

This category is designed for intellectual property rights holders, including trademark, patent or copyright owners, or their agents (agents may include legal representatives, trade associations, data aggregators and brand protection companies) who need to investigate and enforce their intellectual property rights. It also may apply to OpSec actors who address brand-based phishing that facilitates criminal theft, product counterfeiting, etc. 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.

Legitimate and lawful purposes for access include:

- Investigating, tracking and preventing intellectual property infringement
- Researching and investigating intellectual property infringement trends
- Contacting infringing parties and relevant service providers
- Identifying domains to support IP enforcement
- Initiating or facilitating administrative proceedings
- Maintaining intellectual property rights

Examples of investigation and enforcement activity include:

[4] ICANN's IPC has been asked for additional detail regarding eligibility in this category.

- Preventing consumer confusion, theft and fraud and other crimes (e.g., counterfeiting) through infringement of trademarks
- Preventing the unauthorized distribution of copyrighted material
- Responding to trademark related claims
- Trademark clearance
- IP evaluation and investigation

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 agree to follow vetting and accreditation processes (see below).

Examples of entities in this category include: Intellectual property attorneys, in-house corporate counsel, agents/staff of attorneys.

3. Public Safety and Health Organizations[5]

Eligible entities include not-for-profit organizations that seek to protect public safety and health. These are organizations which are formally organized under the applicable laws of the country in which the organization is based, and which have identified their missions (as specifically identified in their documents or organization, such as bylaws or articles of incorporation) as specifically encompassing one of the following: academic and other non-profits with legitimate or legal public safety or health purposes; child protection and child anti-abuse organizations; combating human trafficking; combating counterfeit pharmaceuticals; combating dangerous counterfeit products; and combating hate, racism and discrimination.

Legitimate and lawful purposes for access:

- Investigating, tracking and preventing activity that is dangerous to public health or safety
- Researching and investigating trends related to public health or safety threats
- Contacting victims of activity that is dangerous to public health or safety
- Identifying domains that may be involved in activity that threatens public health or safety
- Providing reports related to public health or safety threats to a government agency or law enforcement
- Initiating or facilitating legal proceedings

[5] There are a range of non-governmental organizations which serve a public health and safety function. For the purposes of clarity and certainty, this section has focused specifically on those organizations which have a mission of combating threats to public health and safety.

Examples of categories that are addressed through investigation and enforcement of applicable law include:

- Fraud
- Theft
- Child abuse
- Human trafficking
- Sale of dangerous and illegal goods and substances
- Hate, racism and discrimination
- Terrorism and threats to national security

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 agree to follow vetting and accreditation processes (see below).

Examples of entities in this category include: The Internet Watch Foundation, NCMEC, LegitScript, The Southern Poverty Law Center, the Anti-defamation League, Human Rights Watch, Amnesty International, and the Red Cross.

4. [Placeholder for Other Potential Purposes]

This section captures additional suggestions that need to be fleshed out and considered for future inclusion. Contributors to this section are asked for additional detail regarding eligibility in this category (e.g., who needs access, how Eligible Entities will be identified, what credentials Eligible Entities may present, etc.).

This category is designed for organizations that conduct compliance and verification activities to help avoid fraud or other harms. Eligible Entities include companies, or individuals at companies, who provide investigations, due diligence, and legal compliance services for their company or another corporation, or provide it as a solution and/or service to other individuals, entities or end-users. Agents may include academics, legal professionals, accountants, ~~journalists~~ and others that need to conduct due diligence for themselves or on behalf of others.

Legitimate and lawful purposes for access include:

- Investigating fraudulent use of registrant’s name in domain name registrations
- Asset investigation and recovery
- Locating a person for service of process
- Identifying parties and non-parties
- Contacting a registrant’s legal representative

- Taking legal action or responding to legal action (e.g., court, administrative or arbitration proceedings)
- Performing contractual compliance and due diligence investigations
- Conducting registration data escrow audits and other regulatory and contractual audits
- Validating site ownership and eligibility to conduct commercial activity
- Proving ownership in domain name purchase/sales transactions, brokering and escrow
- Transferring a domain name between registrars or registrants

Examples of services covered include:

- Validating site ownership to ensure transparency and accountability for commercial activity
- Investigating and reporting on fraudulent uses of domain names
- Investigating asset location and recovery
- Initiating or responding to a legal action
- Providing escrow services
- Transferring domain names between registrars or registrants
- ~~Journalistic investigation of domain name issues or trends~~

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

Applicants must agree to follow vetting and accreditation processes (see below).

Examples of entities in this category include: Escrow.com and Payoneer (Escrow service providers), Sedo.com and Godaddy's Afternic (Secondary Marketplaces), Heritage Auctions Snapnames, and Namejet (Auctioneers), Lazard, Morgan Stanley, Goldman Sachs, Barclays (M&A advisors); Hilco Streambank, Berggren, Media Options, BrandIT (IP and Business Brokers); EY, PWC, Deloitte, KPMG (Accounting / Trustees and Receivers), Dentons, Norton Rose (law firms and paralegals).~~ Examples of investigation related entities include NYT, Washington Post~~. Examples of research related entities include Carnegie Mellon University, Berkman Centre for Internet & Society at Harvard University and Oxford Internet Institute.

Validation and Review of Access Purposes

Accreditations for Eligible Entities will be subject to periodic review to ensure they meet the access purpose criteria. As discussed further below (see Logging), logging should allow analysis of access to non-public Whois data to enable detection and mitigation of abuses and imposition of penalties and other remedies for inappropriate use.[6] Appeal mechanisms will apply in the instance that a review results in de-accreditation.

Process for Vetting and Accreditation[7]

Users are to be vetted by the accreditation authority[8] based on credentials presented. Contracted parties are not expected to perform vetting.

Commented [A1]: Contracted parties input: We will require additional detail around which organizations can realistically serve as accrediting bodies, how a given party is determined to be eligible for accreditation, and the criteria by which those parties and their respective credentials are evaluated by the accreditor.

Furthermore, contracted parties will also need to be able to ascertain which users become accredited, and which users access which data and for what purposes -- thus making a system that allows user groups to share credentials very difficult to adopt.

All Eligible Entities must:

- Have a specific purpose for their access to and use of non-public data
- Certify that access to and use of non-public data is for a legitimate and lawful purpose
- Swear under penalty of perjury that they will not intentionally misuse the non-public data entrusted to them
- Comply with applicable laws (e.g., GDPR) and terms of service to prevent abuse of data accessed
- Be subject to de-accreditation if they are found to abuse use of data
- Be subject to penalties under applicable laws (e.g., GDPR);
- Submit an application with verifiable:
    - Contact details
    - Name
    - If Applicant is an agent, the name of individual or entity for whom agency exists
    - Physical Address
    - E-mail Address
    - Telephone number
- Submit required documentation:
    - Cybersecurity & OpSec Investigators:
        - i) Verifiable credentials[9] and, in the case of agents, a Letter of Agency, Letter of Authorization, or Power of Attorney document authorizing action on behalf of an Eligible Entity (e.g., Power of Attorney documenting ability to act on behalf of an intellectual property owner).
    - Intellectual Property Protection:
        - i) Evidence of IP ownership or a Letter of Agency, Letter of Authorization, or Power of Attorney document authorizing action on behalf of an Eligible Entity (e.g., Power of Attorney documenting ability to act on behalf of an intellectual property owner).[10]
    - Public Health and Safety Organizations:

Commented [A2]: Contracted parties input: Contracted parties believe that in the case of IP rights holders, simply demonstrating ownership of a trademark registration or copyright is not sufficient to qualify that party to access non-public Whois data and that additional credentials, along with a specific and valid purpose, will likely be necessary.

[6] Much like the "Purpose-Driven Access" model proposed in the EWG Report, p. 10

[7] Note additional scenarios for accreditation - *Id.* at 63

[8] This responsibility could fall to a trusted third party, similar to Deloitte administering the Trademark Clearinghouse.

[9] We look to the security community for more information about credentialing; the APWG has offered to form an expert working group with FIRST and M3AAWG to assist ICANN with this process. (Letter submitted by APWG -- posting pending at ICANN)

[10] We look to the IPC for more information about credentialing.

i) Articles of incorporation or bylaws that specify that the mission of the organization encompasses a public health and safety purpose;
ii) Evidence of the organization's activity in stated area(s) of practice; or
iii) Letters of endorsement, accreditation or membership of a recognized agency, legal authority, or NGO alliance (such as the European NGO Alliance for Child Safety Online, the Child Exploitation and Online Protection Command, the United Nations Human Rights Council, or similar).

○ Other organizations: [TBD][11]

- Undergo validation by an ICANN-approved agent (similar to the services offered by certificate authorities or those offered by Deloitte for the trademark clearinghouse)

Once the Eligible Entity successfully completes the above steps, the ICANN-approved accreditation authority issues one of two decisions:

Application is accepted and the applicant is issued credential
- Or -
Application is rejected

Accredited parties must renew their accreditation annually. Renewals will 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. Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation. The accreditation authority reserves the right to update what credentials or other material are required for accreditation.

Proposed Operating Model & Temporary Access Protocol

The operational aspect of the accreditation and access model proposed here is a pragmatic solution for interim compliance with GDPR and can be implemented by May 26, 2018 with minor modifications to existing systems. The proposed approach would allow gated access to non-public Whois data while achieving the goals of:

- Uninterrupted service
- Maintaining the existing Whois system to the greatest extent possible
- Simplified and consistent implementation
- Centralized logging

[11] Contributors to this section are asked for additional detail regarding documentation in this category.

Later, as efforts to implement RDAP or the new RDS (through the RDS PDP process) emerge, the methods for access to non-public Whois data for lawful and legitimate purposes may also evolve.[12]

Under this proposed approach, once accredited, access to Whois data should be administered by ICANN, who would be responsible for delivering to the contracted parties information regarding the accredited entities or individuals in a timely manner.

Accredited User Access and Whois Providers

Upon accreditation, users are given credentials to access Whois data. Users can present their credentials to ICANN to include their IP address(es) in a whitelist. The whitelist should be operated by ICANN and administrated via the existing RADAR system. Contracted parties validate requesting IP address with the centralized list of whitelisted IP addresses, and are then able to deliver access to single record queries and automated access via port 43.

Individual Queries

In addition to the web based lookups offered by registries and registrars, ICANN should continue offering WHOIS lookups for non-public data to those who have credentials. Both can use a simple, centralized, expedient and low-touch implementation tactic to provide access.

1) Leverage and extend the existing ICANN centralized Whois system (as hosted on the ICANN website here). Contracted parties provide ICANN with full, unlimited access to non-public Whois data via Port 43. Credentialed users submit individual queries from their whitelisted IP address(es) to the ICANN query mechanism and are granted access to individual non-public Whois records.
2) Leverage and extend existing web-based access provided by contracted parties. Contracted parties provide credentialed users the ability to submit individual queries from their whitelisted IP address(es) to their web-based form and grant access to individual non-public Whois records.

Temporary Access Protocol for Higher-Volume Queries

A similar Temporary Access Protocol should be developed and implemented for volume Whois queries until such time that RDAP is implemented across all contracted parties. On May 25, Port 43 will display the full non-public WHOIS record, but will be closed to public use and accessible only by whitelisted parties and ICANN. Credentialed users and systems can then access non-public Whois data via Port 43 using automated means.

[12] Future updates could also include an anonymized or “tokenized” system whereby a data processor anonymizes data fields containing personal information -- replacing that information with consistent tokens across all Whois records in all Whois databases so that queries issued by accredited bodies can detect patterns of abuse without having access to the broad base of personalized data and need only then request reveals of personal data directly related to tokens triggered by the purpose of their search.

Logging[13]

The query activity of all accredited entities will be logged by the entity that provides access to the Whois queries. Logs will include accredited entity, purpose, query, and date. Logs must be retained for a two-year period in a machine-readable format and 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. Each query must be mapped to a purpose that is applicable. These steps will allow for auditing of 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. Similar to what was proposed in the EWG Report, auditing will encourage accountability regarding use of gated data for designated purposes only.[14] Note that appropriate restrictions to logs should exist -- as the EWG Report stated: "Access to ... logs must be restricted to those trusted, authenticated, authorized individuals and entities with a specific purpose and 'need to know.' … [including] (to monitor RDS compliance with data protection legislation.)."[15]

Abuse Reporting

The system will be suitably transparent to allow appropriate access to third party examination of query rate and volume. A mechanism will be provided for reporting to the accreditation authority over-extensive use, mirroring or other abuses, for the purpose of revoking accreditation.

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, contracted parties may, at their own expense, demand an audit of any accredited entity. A contracted party'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 Principles[16]). Also, query logs should cite purposes of access, which must be tied to a legitimate and legal use for each accredited user's 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 an accredited party. Audit scope may include a request for correspondence sent by accredited entities to registrants as a result of access and use of non-public Whois data to validate that access and use of non-public data was not for illegitimate purposes (e.g., spam).

Fees and Renewal

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

[13] Logging responsibility decision must be deferred until the technical implementation of the Whois query mechanism is decided -- if contracted parties receive queries, they will have responsibility, if using the ICANN centralized Whois -- they would be responsible for logging.

[14] EWG Report, p. 91

[15] *Id.* at 116

[16] *Id.* at 94

users for each accredited entity. Contracted Parties and agents should need minimal support to integrate this authorization system into their workflow for access to non-public Whois data.

Complaints

- Complaints regarding accuracy of data will be addressed directly to the domain name's sponsoring registrar for resolution.
- 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 relayed to the accrediting agency for appropriate remedial action (see following sections on Penalties and Data Misuse Penalties).

Penalties

An auditing agency will audit non-public 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 are applied to different purposes. Violation of terms and conditions may result in graduated penalties (such as restricted/throttled access, or denial of further access -- see following section on Data Misuse 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 acting on the behalf of companies or individuals who have legitimate use of the data 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.

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 and applicable law.

Commented [A3]: Contracted parties input: This level of unlimited access raises significant concerns with regard to the data minimization principle of the GDPR and the principle that processing (including disclosure) of personal data should be limited to that which is required to meet a specific and legitimate purpose.

Contracted parties encourage the authors to consider the ways in which the to-be-accredited parties use Whois information and whether those uses can be served by a subset of the data, by anonymized data, or through means other than the Whois.

Data Forwarding

It will not be permissible to forward data to another party (whether accredited or not) except as allowed under applicable law. Users will agree as such via the terms of use and code of conduct.

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 (unless acting as an accredited agent)
- Use of data for a purpose that is inappropriate for the accredited user type

Data Misuse Penalties

In the event of breach of the terms and conditions, any accredited user's right to access, retain or use data may be suspended.[17] Upon being notified of a breach, a user's access privileges may be revoked, in which case that user must delete any retained data and provide notice to the auditing agency that the data has been deleted. Data misuse violations may be appealed to accrediting body (see EWG Report, RDS User Accreditation Principles[18]) and access may be reinstated at the discretion of that body.

Commented [A4]: Contracted parties input: Contracted parties are concerned by the lack of detail as to how misuse will be identified and monitored, beyond just providing an abuse reporting mechanism. In order to minimize the liability to which contracted parties may be exposed, we believe more proactive monitoring -- and subsequent enforcement -- of data misuse is necessary. In all cases, the decision to revoke or suspend credentials and/or access to non-public Whois data must reside with the applicable contracted party. Further, contracted parties reserve the right to report users who abuse the data to the appropriate DPA for investigation, and should have the right to invoke penalties in cases of misuse.

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

[17] Further, depending on the nature of misuse, GDPR penalties may apply.

[18] *Id.* at 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 report[19] and ICANN’s Cookbook,[20] 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:

1. Providing access to accurate, reliable, and uniform registration data in connection with the legitimate interests of the registrar and Whois system stakeholders;[21]

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

[20] The Cookbook, Section 7.2.1, at 34. **https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf**

[21] GDPR Art. 6(1)(f)

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:

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

Business/Personal Domain Name Purchase or Sale	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.	Prerequisite for functioning marketplace for DNs	-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	Registrants, potential DN buyers, resale agents, Registrars

Technical Issue Resolution	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	Providing security and stability of the DNS, consumer protection, and protection of Registrants expectation of service Providing a pathway for resolving technical problems/ issues	- Validation of Registrant information -Provision of access to technical users. -Foregoing requires storage of access to technical contact information	Registries, Registrars (Network Operations); DNS service providers; cybersecurity experts

	address various kinds of issues – for example, postmaster for email issues.)			
Domain Name Certification	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 about the Registrant.	Protecting registrant's interest in maintaining secure DN Providing consumer protection and security	Validation of registrant contact info for EV, DV, OV SSL certifications -Foregoing requires storage of and access to full Whois data	Certificate Authorities, SSL Certification providers, Registrants, Registrars

Individual Internet User Protection Security and Trust	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.	Safety, consumer trust and protection, validation of trustworthiness of the information provider.	-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 - Ensuring identity and organizational affiliation of websites conducting commercial activity like accepting credit card or other electronic payments or placing advertisements & promotions	Consumers , online platforms, and the general public

Academic/ Public Interest DNS Research	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.	Promotes broad range of research purposes to improve function, use security, and stability of the DNS; Supports freedom of expression and academic research	- Access to public data and certain non-public data in anonymized form. - Foregoing requires the storage, publication and access to Whois data	Students, research orgs, ~~journalists ,~~ and academics

Legal Actions	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.	Investigating and remediating possible IP infringement or other civil law violations -Preventing fraud and other forms of abuse -Facilitating the establishment, exercise, or defense of legal claims	-Disclose to third party IP rights owners; potential legal complainants - 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. -Foregoing requires the storage, retention, publication and access to the full Whois data; enabling reverse Whois lookup	IP lawyers; intellectual property owners, brand protection and enforcement services companies and associations; cybersecurity experts; Registrars; Registry Operators

Regulatory and Contractual Enforcement	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	-Supports audit and enforcement of private and public legal obligations -Supports security, stability and trustworthiness of DNS	-Storing and disclosing data to regulators, ICANN and authorities entrusted with domain name dispute adjudication. -Foregoing requires storage, retention and access	Regulators, ICANN Compliance, Parties to contracts, Administrative and enforcement entities such as WIPO

	telephone number, as appropriate for the stated purpose. For example, ICANN approved domain name dispute resolution providers need access for domain name dispute resolution.		to Whois data.	

Public Health and Safety Protection and Criminal Investigation	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	Public health, safety and security Investigating cyber- crimes and cyber-enabled crimes;	-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 -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 -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 -Foregoing requires storage, retention and access to full Whois data; enabling reverse Whois lookup to determine	Law enforcement and government or private entities entrusted with enforcement responsibilities; public health and safety organizations, including victim advocacy organizations; digital crime/abuse teams.

			breadth and scope of abuse and properly identify person/entity responsible for abuse and/or criminal activity.	

DNS Abuse Study, Investigation and Mitigation	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. 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.	Protecting Registrant from abuse and hijacking of Registrant's DN Consumer trust in the Internet Ensuring network and information security and stability of the DNS Combating unlawful or malicious/abusive actions negatively affecting secure and stable functioning of the DNS	-Providing access to Registrant data for the purposes of detecting and mitigating DNS abuse -Foregoing requires storage, retention, publication and access to Whois data; enabling reverse Whois lookup	Law enforcement and public safety agencies; Cybersecurity firms and individual cybersecurity analysts and experts; Online platforms Registry Operators, Registrars ICANN Compliance

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

Draft Accreditation & Access Model
For Non-Public Whois Data
April 20, 2018
Annotated Version 1.4

ANNEX B

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 stay as close as possible to the current Whois system and the current thick Whois policy -- while finding a solution that complies with GDPR.

As part of that compliance effort, ICANN Org has proposed a model for the Whois system that limits public access to Whois data. This model, without a mechanism for access to non-public Whois data for legal and legitimate purposes, would effectively disable a critical tool employed for the safe and stable operation of the DNS, the prevention of crime, conducting vital cybersecurity operations, the protection of consumers, the enforcement of intellectual property rights and other critical functions[22]. By ICANN's own proposed timeline, access to Whois would not be implemented until December 2018 or later -- causing a prolonged Whois access outage.

This is a significant problem, considering:

- Bad actors operate at a global scale, across multiple registrars and top-level domains, sometimes using thousands of names in coordinated and automated attacks.
- Harms range from consumer fraud, disinformation, spam, phishing, botnet attacks, and distributed denial of service (DDOS) attacks to the grimmer, including human trafficking and child abuse.
- The harm inflicted is dangerous, disruptive and expensive, and prevention or remediation windows are often measured in seconds or minutes, not days or weeks. The consequences of inaction or impaired action can be disproportionate, dire and irreversible for Internet users worldwide.

Whois data elements, which are collected in conjunction with a domain registration contract, 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 of jointly controlled and/or connected domains that are 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 in the first instance.

[22] Historical information (see http://forum.icann.org/lists/gnso-dow123/docfMF1nFg7Zy.doc) affirms that Whois data is not meant to be constrained to use only in resolving technical issues, but "rather to allow any person to contact any other person who had obtained an online address, regardless of purpose."

Moreover, ICANN org's proposed model will severely impair or prevent crucial legal verification, investigation, compliance, and rights enforcement obligations, which are critical to the protection of the public. For example:

- Companies, and their agents who perform due diligence, compliance, and verification in connection with the acquisition or disposition of assets, bankruptcies and receiverships, and related professional services, will have their ability to comply with obligations impaired or prevented.
- Consumers will face fraud and domain name theft as a result of the inability of secondary domain name marketplaces and escrow services to verify and investigate domain name transfers and transactions, thereby resulting in greater instances of fraud, theft and identity theft.

As a result, governments, law enforcement, businesses, intellectual property owners and Internet users worldwide have expressed concern. ICANN's Governmental Advisory Committee has given consensus advice to the ICANN Board in its ICANN 61 communique to maintain Whois to the fullest extent possible and to mandate an access mechanism to non-public Whois data. This view is also held by the Intellectual Property Constituency, the Business Constituency, and the At-Large Advisory Committee within ICANN, as well as other global entities and sectors outside of the ICANN community.