**WHOIS Technical Requirements Survey**

**Final Report**

**STATUS OF THIS DOCUMENT**

This draft final report explores the WHOIS Survey WG recommendations regarding a survey conducted about possible technical requirements of a future Domain Name Registration Data solution. Prior to delivery of the report to the GNSO Council, a public comment forum will be made available to the community for input into the final report.

**SUMMARY**

This final report is published in response to a request from the GNSO Council pursuant to a resolution adopted on 6 October 2011 (see – Motion 8 at <http://newgnso.icann.org/meetings/minutes-council-06oct11-en.htm>).

**Table of Contents**

[1. Executive Summary 3](#_Toc346891370)

[2. Objective and Next Steps 4](#_Toc346891371)

[3. Background on WHOIS Technical Requirements 5](#_Toc346891372)

[4. Survey Results Analysis 7](#_Toc346891373)

[5. Working Group Recommendations 30](#_Toc346891374)

[6. Next Steps 31](#_Toc346891375)

[Annex 1 - TBD 32](#_Toc346891376)

# Executive Summary

**1.1 Objective**

* The objective of this report is to

**1.2 Background**

* As a prerequisite for this report

**1.3 Survey Results Analysis**

* Placeholder

**1.4 Working Group Recommendations**

* Placeholder

**1.5 Next Steps**

* Placeholder

# Objective and Next Steps

This report is published in response to a request by the GNSO Council for a report and analysis of survey about possible technical requirements of a future Domain Name Registration Data Registration Service (DNRD-DS). The objective for the Working Group is to develop a set of proposed recommendations around the measurement of support of proposed technical requirements.

This report will be made available for public comment prior to the WG’s delivery of the final version to the GNSO Council for their consideration. After which, the Council will decide next steps, if any.

# Background on WHOIS Technical Requirements

In May 2009 the GNSO Council asked ICANN Staff to compile a comprehensive set of requirements for WHOIS that included known deficiencies in the current service and “any possible requirements that may be needed to support various policy initiatives that have been suggested in the past”. This effort was started given the wide community discussions about WHOIS given its history and capabilities to meet expansion demands like Internationalized Domain Names (IDN), Registry Registrar operations, and efforts by the Internet Engineering Task Force (IETF). ICANN Staff produced a report compiling an Inventory of WHOIS Service Requirements on 29 July 2010 and delivered the report to the GNSO Council for their consideration. The report essentially distilled policy discussions and other activities, into technical requirements that would be necessary to correct deficiencies and implement various policy proposals. The report was not intended to define or suggest the policies or operational rules that should apply, but only a technical inventory of requirements that may address policy issues.

After deliberation by the GNSO Council, it was [resolved](http://gnso.icann.org/en/council/resolutions#20111006-1)[[1]](#footnote-1) on 6 October 2011 that the GNSO convene a Working Group of interested volunteers to draft, implement, and analyze the results of a survey measuring the level of support for various technical requirements as outlined in the final Inventory of WHOIS Service Requirements Report of 29 July 2010. The WHOIS Survey Working Group (WSWG) formed shortly after the GNSO Council resolution and drafted its [charter](http://gnso.icann.org/issues/whois/charter-wswg-06oct11-en.pdf)[[2]](#footnote-2) instructing the WG to describe the results of a survey and recommendations for next steps for the GNSO Council’s consideration concerning the WHOIS service requirements.

After eight months of drafting effort, the WG produced a draft version of the technical requirements survey and opened a [public comment forum](http://www.icann.org/en/news/public-comment/draft-whois-requirements-survey-30may12-en.htm)[[3]](#footnote-3) to solicit feedback from the community. All feedback was submitted through the draft survey itself as hosted by the open-source survey software of Lime Survey. Each comment was reviewed by the Working Group and if adopted, the suggested change was incorporated into the final version of the survey. After consideration of community input and the implementation of the Lime Survey software within the ICANN IT infrastructure, the survey was made available to the community on 13 September 2012.

The survey consisted of 15 sections around the 11 technical requirements defined in the inventory report, and it was made available to the community until 31 October 2012. The survey was lengthy and therefore the option to create an ID and return to the survey at a later time was made available. Many sections of this survey required a high degree of technical skill around WHOIS and in some cases participants either did not complete the survey, only completed answers they felt they could answer leaving difficult one blank, or reached out to colleagues with technical skill to complete it. Statistics of the survey reach can be found in the next section, as well as, an analysis of service requirement results in the subsequent sections of this report.

#

# Survey Results Analysis

**4. 1 Background on the process**

<<placeholder>>

Response summary

Total responses:247

Full responses:67

Incomplete responses: 180 (20 Saved, not submitted)

**4. 2 R0 - Participant Profile**

In development of the survey, the WSWG felt it was important to gauge certain attributes about the survey participants as it may be a valuable reference in analyzing the various technical requirements. Such attributes that were measured include:

* Affiliation and size of the organization
* County location
* Experience with registration of domain names
* General Purpose for accessing and using Domain Name Registration Data Directory Service (DNRD-DS)

**Summary of Results:**

In review of the 67 completed responses, it appears that the participants ranged widely across affiliation and organization size. Commercial and non-commercial organizations types of entities are well represented, in addition to the largest respondents belonging to contracted parties. Governmental organizations were the one entity type not represented among the participant pool. Organization size of the participants was predominantly organizations of 50 persons or less, however responses from medium and large companies did occur.

Location of the participants was another attribute tracked. 45% or 35 of respondents were from the United States, while the remaining was international. The second largest pool was from European countries.

Virtually all respondents had experience with registering both ccTLD and gTLD domain names. However, a little less than a quarter of them selected an answer of “Not Applicable.” It is difficult to specify the reason for this answer, but it is suspected that good portion of these responses pertain to contracted parties. The purpose of domain registrations was fairly balanced across commercial, non-commercial and personal.

Nearly 75% of the respondents access DNRD-DS services weekly to multiple times during a day with just over 60% accessing via “Direct server query access.” 30% or 20 of the participants accessed the services like Domain Tools or Registrar/Registry services via a web browser.

Participants were asked what were the reasons or the most beneficial uses of DNRD-DS:

|  |  |  |
| --- | --- | --- |
| **Answer** | **Count** | **Percentage** |
| To determine if a specific domain name is unregistered or available (1) | 34 | 50.75%   |
| To find out the identity of a person or organization responsible for a domain name or web site (2) | 54 | 80.60%   |
| To support technical operations of ISPs or network administrators, including tracing sources of spam or denial of service attacks (3) | 31 | 46.27%   |
| To identify the owner of a domain name for consumer protection or intellectual property protection purposes (4) | 27 | 40.30%   |
| To gather names and contact information for marketing purposes (5) | 3 | 4.48%   |
| To support government law enforcement activities (other than intellectual property) (6) | 8 | 11.94%   |
| To monitor and manage groups of domains for self or on behalf of others (7) | 14 | 20.90%   |
| Other | 7 | 10.45%   |

Other responses:

* To identify a contact address (preferably email) for the domain holder (I don't care about their "identity" merely their contact details)
* Investigation
* Transfers
* Check our WHOIS-service
* Scientific research about the Internet
* For Verification purposes
* To facilitate inter-registrar transfers
* To find IP address of name server

34% or 23 of the Respondents stated they maintain a DNRD service as a Registrar, Registry Operator or a Regional Internet Registry. Over 80% of these responses stated that the service was custom developed in-house over using open-source solutions. The following names were listed as solutions used:

* mod\_whois
* anadol
* internic.net
* Windows
* RIPE WHOIS
* net4 Whois server
* pwhois
* ATLAS
* whois.denic.de

**4. 3 R1 - Provision of a publicly accessible and machine parsable list of domain names**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 4 R2 - Definition of a Standard Query Structure**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 5 R3 - Definition of a standard data structure for WHOIS responses**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 6 R4 - Definition of a set of standardized error messages and standard handling of error conditions**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 7 R5 - Submitting WHOIS queries for domain names**

Searching Domain Name Registration Data Directory Service (DNRD-DS) provided by Registrars or Registries is offered by searching the domain name data element only. The WHOIS Technical Survey R5 question measured the interest of expanding search queries of Domain Name Registration Data (DNRD) beyond the domain name. Survey respondents were also presented expanded search options of language and technical capabilities to gauge significance of advanced services.

**Summary of Results:**

Of the survey respondent replies, 67 completed the section fully, whereas 177 respondents did not fully complete this section. Over 53% respondents of fully completed surveys indicated positive interest in advanced search options of DNRD; whereas, nearly 30% stated it was unnecessary. There were 12 incomplete surveys which also favored the advanced search options as opposed to 4 unnecessary and 8 “no answer.” A “no answer” assumes the respondent is indifferent making the incomplete responses irrelevant. Generally, there is interest to expand search options. However, considering only slightly more than half of the fully completed surveys answered “Yes” and nearly 30% answered “No”, advanced searching of DNRD is not overwhelmingly supported.

**Key Findings:**

53.8% Survey respondents answered “Yes” to advanced searching of DNRD beyond domain name. When ranking the priority of searchable data elements, domain name ranked highest by 36 question respondents. Resulting, the current searchable DNRD-DS meets the need of over half of respondents requesting advanced search options.

Priority of other searchable data elements ranked Name Server, Contact Name, Contact Email sequentially second, third and fourth of importance. Other data elements, such as registration dates and contact addresses were equally weighted by respondents.

Other advanced search options indicate a general interest to expand beyond limitation of current options. When questioned if Boolean (AND, OR, NOT) search options were important, most respondents answered “Yes”. There is also interest to search DNRD via wildcard (a wildcard is a character that may be substituted for any of a defined subset of all possible characters). Over half respondents affirmed searching DNRD in native language (non-ASCII) format is needed. There were qualifying statements by respondents that much of the advanced search options should be restricted to specific data elements and audience.

**4. 8 R6a - Adoption of a structured data model for WHOIS data**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 9 R6b - Extending the currently defined set of registration data elements**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 10 R7 - Internationalized Registration Data Requirements**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 11 R8.1 - Defining an authentication framework for WHOIS**

The current Domain Name Registration – Data Services (DNRD-DS), commonly referred to as WHOIS, allows public access to registration data with limited, if any, authentication protocols. It is debated if greater controls to Domain Name Registration Data (DNRD) should be implemented. Authentication protocols could benefit in managing who has access to the data, allow auditing of the access and enable segmentation of audience and data. There is an inherent cost of enforcing an authentication framework to manage the access controls and risk legitimate access to be hindered.

The WHOIS Technical Survey set out to define an authentication framework for WHOIS service that is able to accommodate anonymous access as well as verification of identities using a range of authentication methods and credential services.

**Summary of Results:**

Survey participants were asked if access to DNRD should have better controls. Over a quarter, 17 of 67, of the respondents indicated there is no need for elevated access. The balance, 40 participants or about 60%, agreed to allow elevated access to certain audiences for reasons based on their role and/or geographic location, due to privacy laws. The support for increased access controls is evident. The policy of authenticated access will need definition as the respondents clearly have varying positions of who, what and how controls are adopted.

**Key Findings:**

Although the question of who should have access based on need was widely disbursed in support, when questioned if controls around the Top Level Domain (TLD) are necessary, nearly 45% indicated there were indifferent or it was not necessary. That could be deciphered two ways. Either the access controls need to be broad-based, not circumscribed; or, it is more relevant who is asking for the data than the data, and specifically TLD, itself.

There was overwhelming support for type of access, security and rate limiting controls. Of the 67 respondents, over 36% chose elevated access rights should be granted to people (human-use) only. Another 30% agreed to people or computer access. But, less than 5% selected computer only elevated access rights. It is evident the respondents do not want automated elevated access.

Many respondents indicated access to DNRD should be secured. About 40%, however, indicated no preference or no answer. Those that did support secure access the majority, 35%, selecting SSL (secure socket layer) as the preferred method.

The most notable response to the survey was the tremendous support of rate limiting the access. Over 66% of the respondents confirmed rate limiting is required in an effort to manage the DNRD-DS service. Considering the low percentage of respondents agreeing to computer-only authenticated access and the high percentage of rate limiting controls, it is clear there is concern over automated processing and potential abuse.

**4. 12 R8.2 - Implementing an authorization framework**

Discussions of segregated access to DNRD have been ongoing within ICANN. The approaches discussed have been varied. The common theme being restricting unfettered public access to DNRD as is currently available. The discussions have taken place within ICANN groups. The WHOIS Technical Survey’s intent to broaden the audience to participants, not involved in the ICANN activities. The goal to gauge wider community support of implementing an authorization framework that is capable of providing segmented access.

**Summary of Results:**

Survey respondents agreed, by over 58%, to a systematic, policy driven approach to segmented access to DNRD. This could be segmented by access to specific DNRD data elements or user segmentation to DNRD-DS. There were many statements that this needs to be driven by policy not protocol. Considering the strong support of segmented access, there was not a clear response to degree of importance nor was it required in respondent’s jurisdiction. In conclusion, although survey respondents support implementing an authorization framework, further due diligence on the necessity of it is required.

**Key Findings:**

Almost 60% survey respondents agreed DNRD-DS a permissioned based access should be standard operating procedure. The question positioned this to be determined, and governed, by policy. That statement was strongly supported in respondent comments.

Respondents were presented the position of enacting login mechanism for all DNRD-DS users, regardless if DNRD-DS services are open or anonymized. The results were inconclusive with nearly equal response in favor and against.

Although segmented access was strongly supported, when challenged to rank on importance, respondents ranked it nearly equally distributed between Most to Least, 1-5. The mean average was 2.84 between respondents. This indicates although access controls are supported it is not a top priority by survey respondents.

Local jurisdictions did not win out on claim of granulated access. Over 50% of completed responses had no answer. It is not relevant to local laws of the respondents. The survey either did not reach the audience with greater privacy laws in their jurisdiction or current services meet their needs for control of access to DNRD.

**4. 13 R8.3 - Defining a framework and baseline set of metrics**

With an authentication service in effect, it offers the ability to audit and report of access. Auditing could benefit many stakeholders. Managing the DNRD-DS Registrars and Registries can be improved by monitoring and regulating systems. Domain owners could benefit of auditing and reporting access to thwart potential hijackers. When segmented access is available, along with reporting and tracking, it is conceivable it can be abused or could create additional challenges to the very stakeholders protecting the consumers. Any framework needs to consider baseline set of metrics that can accommodate future policy development for auditing that meets the needs of all stakeholders.

**Summary of Results:**

This survey section presented participants options to select data elements worth collecting if a framework was in place. There were 67 completed surveys, 177 incomplete. Of the incomplete surveys, 8 or less responses were given in any one question, making the incomplete responses mostly irrelevant.

Most data elements received a healthy response to collecting data by the survey respondents of the completed surveys. It is evident there is interest and support for a framework that allows data collection, retention and tracking of DNRD-DS. Simultaneously, it needs to be recognized this could cause issues of security concerns. Any framework established will need to have a well-defined policy of method of access and use.

**Key Findings:**

Survey respondents largely found most every data element presented worth collected for auditing and tracking purposes. The most supported elements to track were the domain name itself and the data and time it was queried. Both of those scored about 60% with an affirmative response to collect the data. The current DNRD-DS service inherently captures this data when queried. Putting in place an authentication system for this tracking is unnecessary.

The one element with more Should Not Collect over Should Collect was the Name of Requestor, 36% to 30% respectively. In fact, Name of Requestor received the highest amounts of votes of Should Not Collect in this section of the survey. Consider the respondents who found tracking this data element Somewhat Interesting, 15%; one can accept it is an interesting option that will need additional input.

When survey participants were presented the question of privacy or confidentially concerns with collecting data, nearly 50% agreed. Respondents went on to comment that retaining information of requestor or requested data could encounter other data protection law, depending on jurisdictions. It could also prove risky in investigative and security issues. A policy of data retention and controls along with strict constraints is necessary.

**4. 14 R9 - New TLDs operating a thick WHOIS**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 15 R10 - Definition of a standard data structure for WHOWAS responses**

<<placeholder>>

**Summary of Results:**

<<placeholder>>

**Key Findings:**

<<placeholder>>

**4. 16 R11 - Registrars and Registries**

Recommendation R11 of the Inventory Final Report dealt with publishing an abuse point of contact as part of a domain registration record. Drawing upon this recommendation, the survey asked respondents whether it was important that this additional element be included in response to WHOIS queries to registries or to registrars. It also inquired about the main ways in which respondents expected to use the abuse point of contact, and about three alternative methods by which the abuse point of contact could be displayed. Among the 67 respondents who completed the survey, as many as 62 answered at least one question in this section.[[4]](#footnote-4)

**Summary of Results:**

Respondents strongly supported inclusion of an abuse point of contact in WHOIS results, especially at the registry level. While a majority indicated that all of the suggested potential uses for this information were at least somewhat important, the single most strongly supported use was for reporting suspected malicious activity associated with a domain name, with the least support for using the information to report technical problems associated with the domain name. Respondents strongly preferred adding abuse point of contact information to the current registrar or registry information included in WHOIS results, rather than either of the other methods suggested.

**Key Findings:**

1. Abuse point of contact for registry WHOIS (Q. 1111): 61.2% of respondents considered this very important, and another 17.9% thought it somewhat important.

2. Abuse point of contact for registrar WHOIS (Q. 1112): While slightly fewer respondents thought it was very important to include this information in WHOIS results from registrars, a majority (52.2%) did think so. The 74.6% of respondents who thought this feature at least somewhat important in registrar WHOIS results approaches the 79.1% figure for registry WHOIS.

3. Most valuable potential uses (Q. 1113): Clear majorities thought it at least somewhat important that abuse point of contact information be made available in order to report malicious activity associated with a domain name (80.6%), report false or inaccurate WHOIS data (68.7%), report violations of legal rights associated with the domain name (65.7%), or to report technical problems associated with the domain name (61.2%), as well as a catch-all response of making “general use of an abuse point of contact” with such data (71.6%). The highest single figure for a use deemed “very important” was 62.3% for reporting suspected malicious activity; the lowest such figure (34.3%) was for reporting technical problems. (It may be difficult to make meaningful comparisons among the different choices, since the uses were not specifically defined in the survey and may well overlap in the minds of some respondents.) Only a handful of respondents (11.9%) answered that “other uses” not listed in the survey were very or somewhat important to them.

4. Method of including abuse point of contact (Q. 1114): A majority of respondents (55.2%) strongly preferred adding abuse point of contact information to the registrar or registry contact data currently appearing in WHOIS results. Including the “somewhat prefer” responses brings the positive total for this method over 73%, with only one-tenth as many respondents (7.5%) at all opposed to it. By contrast, only 35.8% stated any preference for including in WHOIS results a link to or index into a publicly accessible table of abuse points of contact. Substituting the abuse point of contact for the current contact information was even less popular, with only 22.4% of respondents expressing any preference for this option, which 17.9% of respondents strongly opposed.

# Working Group Recommendations

<<Placeholder>>

# Next Steps

The GNSO Council is now expected to review and deliberate the WG’s Analysis and Recommendations.

<<Placeholder>>

# Annex 1 - TBD

<<Placeholder>>

1. GNSO Council Resolution on WSWG: <http://gnso.icann.org/en/council/resolutions#20111006-1> [↑](#footnote-ref-1)
2. WSWG Charter: <http://gnso.icann.org/issues/whois/charter-wswg-06oct11-en.pdf> [↑](#footnote-ref-2)
3. WSWG Public Comment: <http://www.icann.org/en/news/public-comment/draft-whois-requirements-survey-30may12-en.htm> [↑](#footnote-ref-3)
4. Only one respondent who did not complete the survey answered any questions in this section, so the inclusion of incomplete responses would not change the results significantly. [↑](#footnote-ref-4)