Draft Outcomes Report of the Whois Working Group

STATUS OF THIS DOCUMENT

This is Version 1.2 of the Outcomes Report of the Whois Working Group. It was created following the Whois Working Group on 14 June. It is intended to be discussed and significantly refined during the ICANN meeting in San Juan, 25-29 June, 2007.

TABLE OF CONTENTS

Sections yet to be added:

Introduction

Executive Summary

Background: Formation of the Working Group

Membership, meetings and attendance of the Working Group and its sub groups (in annex)

Introduction

Status of statements in this report and description of consensus-building conventions used

Unless otherwise stated, every statement in this report is an agreed description or assertion of the WHois Working Group. Some statements are preceded by the term '*AGREED'* . These statements are an agreed recommendation of this group. Some statements are qualified by a characterisation of '*SUPPORT'* or '*ALTERNATIVE VIEW*'.

The Working Group used the following conventions to express or move towards consensus:

- **Agreement** – there is broad agreement within the Working Group (largely equivalent to "rough consensus" as used in the IETF)
- **Support** – there is some gathering of positive opinion, but competing positions may exist and broad agreement has not been reached
- **Alternative view** – a differing opinion that has been expressed, without garnering enough following within the WG to merit the notion of either Support or Agreement.

The ultimate authority to determine the level of agreement was that of the Working Group Chair, assisted by the Vice Chair.

SECTION 1 – STRUCTURE AND PROCESSES

This section outlines the foreseen operation of a modified Whois with two underlying assumptions:

1 (a) Registration

Distinction between natural and legal persons

This distinction is operational in the sense that it is not difficult to make, and will not vary much between jurisdictions, though forms of legal persons may display such variation.

AGREED[1]*:* A distinction between legal and natural persons should be made. This distinction relates to an historic fact about the nature of the Registrant.

AGREED[2]*:* 'Retained disclosure' implies the ability of a registrant to nominate an OPoC. The implication of the declaration is that the public display of WHOIS data will be different in the following way:

Legal persons	Full disclosure as in Whois today
Natural persons	Retained disclosure due to ability of registrant to nominate an OPoC[3]

TO BE CONFIRMED/DETERMINED: A natural person may nominate themselves as an OPoC and provide their own full contact details.

AGREED: The distinction should be based on self-declaration by the registrant, at the time of registration, as one either a;

- natural person, or a
- legal person (*eg* company, business, partnership, non-profit entity, association, *etc*.

[1] Agreed and confirmed by WG, 14 June, 2007
[2] Agreed and confirmed by WG, 14 June, 2007
[3] The assumption of Sub Group C was that making a distinction between different types of registered name holders would ultimately result in different Whois results for each type, with full disclosure being similar to Whois output today, and 'retained disclosure' providing less immediate data.

47

48

Distinction between Commercial and Non-Commercial uses of Domain Name

STAFF NOTE: On 14 June, the Chair proposed either moving this section to later in the report and state that it was discussed and deemed impractical, or isolating it as an area for more work on how commercial/non-commercial distinctions could be made and enforced.

For an example of how the report may be structured, see the previous Outcomes Report of the IDN Working Group (http://gnso.icann.org/drafts/idn-wg-fr-22mar07.htm) which assembles 'areas of agreement' and subsequently 'areas of support'. The Whois WG agreed on 14 June to agree the structuring of the final outcomes report at a later date.

On 14 June, the Chair also invited Christopher Gibson to further develop this distinction and its implementation in a practical way.

AGREED[4]*:* This distinction is more problematic as it may relate to a mix of uses or to the future intent of the RNH.

AGREED: If this distinction were to be made, it could be made as a self-declaration at the point of registration in addition to the distinction between legal and natural persons.

AGREED: If this distinction were to be made, *natural persons* could be considered engaging in commercial activities if one of the following indicative criteria is satisfied:

a. The offer or sale of goods or services
b. The solicitation or collection of money or payments-in-kind for goods or services
c. Marketing activities, including advertising or sale of advertising (*eg* paid hypertext links)
d. Activities carried out on behalf of legal persons
e. The collection, storing or processing of personal data, or instructing another legal or natural person to collect, store, process, use, transfer or disclose such data *except* in the exercise of activities which relate exclusively to personal, family,

[4] Agreed and confirmed by WG, 14 June, 2007

domestic or household affairs such as correspondence or the holding of address books for family, friends or professional contacts.

If these criteria were not met, the natural persons might be considered to be engaged in *non-commercial activities.*

SUPPORT: The distinction between commercial and non-commercial activities is not by itself sufficiently clear to be operative, but a set of strict, subordinate criteria might make it operational. A detailed elaboration of these subordinate criteria would need to be achieved for this distinction to be operationalised.

TO BE DETERMINED: Whether a distinction could/should also be made between commercial and non-commercial activities in the use of a domain name.

A combination of the two types of the distinction would produce the following result:

	Commercial activities	Non-commercial activities
Legal persons	Full disclosure	Full disclosure
Natural persons	Full disclosure	Retained disclosure

AGREED: If both distinctions – legal/natural and commercial/non-commercial – were to be made, a matrix of the consequences of self-declaration would appear as follows:

1 (b) OPoC Relationships

AGREED: The OPoC's relationships are defined below:

1 Relationship to RNH

1. OPoC may be the same as the RNH
2. If OPoC is not the same as the RNH, OPoC must agree to OPoC status and responsibilities
3. RNH must authorize OPoC for needed capabilities

2 Relationship to registrar

1. OPoC may be the registrar
2. If OPoC is not the registrar, the registrar must accept instructions from OPoC within the scope of its responsibility

FOR FURTHER DISCUSSION: further work needs to be done on what it means to 'agree to OPoC status' (1.2 immediately above) , what 'OPoC status' means (ibid.), and what 'responsibility' means (2.2 immediately above), and what, if any, implications this raises for other policies such as the transfer policy.

3 Relationship to Proxy Services (if any)

FOR FURTHER DISCUSSION: Different views (SUPPORT)have been expressed:
EITHER Proxy registration should be eliminated in the OPoC setting.
OR: The possibility for proxy registration should be maintained as long as the contact details of the 'actual' RNH could be made available through the 'REVEAL' function.

4 Relationship to ICANN

Some relationship between ICANN and the OPoC is needed for enforcement or compliance purposes.
FOR FURTHER DISCUSSION: What, if any, enforcement or compliance relationship exists between ICANN and the OPoC? And, does this apply to all activities by the OPoC, or only those related to the use of a domain name by a natural person?

Different views (SUPPORT)have been expressed:

: EITHER A relationship between ICANN and the OPoC must be accommodated within existing contacts, e.g. in an amended Registrar Accreditation Agreement spelling out the registrar's default role and requiring it to allow only OPoCs that have the necessary capabilities and relationships.)

OR: OPoCs should be accredited by ICANN.

AGREEMENT: Feasibility of accreditation of OPoCs by ICANN may turn on whether there were many or relatively few entities offering OPoC services.

AGREEMENT: Either way, i.e. if there are many or few entities offering OPoC services, ICANN would have to allocate some resources for OPoC compliance.

1 (c) OPoC Requirements

Three OPoC capabilities were developed as mandatory responses to a legal request from a third party.

Working definition of a legal request: "any communication that is made for the purpose of alleging a wrongful registration or use of the domain name, wrongful activity by the registrant, or a challenge that the registration is not a valid OPoC registration. Examples of such wrongful registration, use or activities include phishing, pharming, cybersquatting, copyright and trademark infringement, and other illegal or fraudulent activities. Such a legal notice should be accompanied by reasonable evidence of the wrongful registration, use or activity."

AGREED: The introduction of the OPOC system would introduce delays for Requesters, compared to the status quo, in communicating with and/or identifying the RNH in circumstances raising "legal issues" (as defined above), and that therefore deadlines for actions by the OPOC should be as short as possible.

NB: See 'Section 3 – IMPLEMENTATION' for a discussion of outstanding implementation issues on access proposals.

FOR FURTHER DISCUSSION: Regardless of what remedy is sought, who will be the actor making that remedy?

TO BE DISCUSSED/DETERMINED: Define the category of "serious cases",e.g. phishing, that require the REMEDY option

.

1 (d) Access to unpublished Whois data

Type III Bulk Access

Ongoing query-based or bulk access to any domain by any requester.

This is the current status quo.

FOR FURTHER DISCUSSION: Would Type III access continue in its present form for the data (full or retained)?

Type 1 Access

Restricted, incident-based. Access is limited to the records of particular domains and/or registrants causing problems at a specific time, wherein a specific request is made to a gatekeeper for each incident. Multiple domains could be included in a specific request.

- This type of access cannot currently be provided via Port 43. It might be provided by legal due process, email or other kinds of exchange between parties seeking access and OPoCs, registrars or LEAs.
- This type of access can also incorporate a two-tiered process in which a manual review process gives certain entities access to an automated query screening

process that would accelerate access to the records of problem domains.

FOR FURTHER DISCUSSION: Is Type I access redundant/the same thing as a request to the OPoC for the REVEAL function?

133

Type II Bulk Access

Query-based access to any domain, but with contractual/legal restriction of queries to the records of particular domains and/or registrants needed to support a specific investigation.

- To be effectively distinguished from Type III access, Type II access must be supplemented with record-keeping and auditing regarding which queries were made by users, and by the ability to sanction users or withdraw access rights when access rights are abused. (*Implementation of accountability measures was not discussed.*)
- Type II access recognises that when LEAs are involved, auditing and record-keeping may be limited or blocked when there are special circumstances such as a national security related investigation.

FOR FURTHER DISCUSSION: How might this work for LEA and or private sector ?

134

135

Type IV Bulk Access

Indirect access for private actors via government agencies.
Private actors obtain access to the shielded information through their respective governments or through an agency designated by their governments where permitted by national law.

This type of access would be contingent on national law, and may as such be outside the purview of an ICANN working group. It may be considered as an option for overcoming restrictions on access imposed by other options.

- In many cases, there will be legal restrictions on whether or how governments or LEAs can pass on private data to private actors.

- Type IV access could be considered a special case of Type I access.

FOR FURTHER DISCUSSION: is this a practical option?

NB: See 'Section 3 – IMPLEMENTATION' for a discussion of outstanding implementation issues on access proposals.

There is a distinction between public law enforcement agencies and private actors seeking access to unpublished Whois data.

Public law enforcement agencies (LEA) are defined as governmental agencies legally mandated to investigate and/or prosecute illegal activity.

AGREED: LEAs should be granted access to data elements not shown in the post-OPoC published Whois.

AGREED: LEAs should be granted at least Type I access. (see text box above on Type I access)

AGREED: Global certification mechanisms for organisations' status as a LEA should be explored in greater detail, but a basic institutional framework may already exist, e.g. Interpol, national agencies.

STAFF NOTE: ICANN staff has engaged expertise to explore the issue of publicly documented and currently used mechanisms for recognition such as mutual legal assistance treaties, and also at what private sector initiatives exist for sharing information. This information will be provided to the WG shortly after the San Juan meeting.

SUPPORT: LEAs should be granted Type II access.

ALTERNATIVE VIEW: LEAs should be granted Type III access, or bulk access.

Private actors are defined as organisations or individuals that are not part of a LEA.

AGREED: Private actors have a right to investigate and litigate against domain name registrants who are violating their legal rights.

AGREED: The high incidence and seriousness of phishing mean that the banking sector mean that special attention is needed for banking sector access to unpublished data.

AGREED: It is possible to certify a bank, and more straightforward to do so than other types of private actor.

AGREED: A solution encompassing all legitimate users is preferable to one restricted to the banking sector, especially as some key targets of phishing such as PayPal and ISPs are not banks.

AGREED: Within the constraints of the OPoC proposal, private actors should not be granted Type III access.

SUPPORT: Private actors should have Type I access.

SUPPORT: Private actors should have Type II access.

SUPPORT: The Working Group should not focus its resources on developing a sector-specific proposal for banks at this time.

> *ALTERNATIVE VIEW*: A sector-specific proposal focused on banks could be used as a model or test case for access by private actors.

TO BE DISCUSSED/DETERMINED:

- Whether private actors need a special mechanism for accessing unpublished data
- How to define and identify parties with a “legitimate need” to access unpublished data.

- Whether a category-based approach could or should be used for defining legitimate third parties, e.g. IP attorneys, government-chartered banks, e-commerce consumers
- Whether access to data by various private actors should be uniform across all types
- Whether private actors should self-certify as legitimate parties to access unpublished data
- If private actors self certify, whether and what kind of *ex post* challenge mechanisms might be used.
- Whether sector-based approaches to access to data could or should be used, e.g. the banking sector.

SECTION 2 – COMPLIANCE AND ENFORCEMENT

This section outlines the foreseen enforcement and compliance aspects of a modified Whois.

2 (a) Registration

It is possible that RNHs might declare themselves as natural persons / not engaged in commercial activities to avoid having a full data set published in the Whois database.

AGREED If the RNH falsely described itself as a natural person/non-commercial registrant, then there needs to be a lightweight challenge procedure.

TO BE DISCUSSED/DETERMINED: What form a challenge procedure might take and what relationship, if any, it might have with the existing Whois Data Problem Reporting System.

2 (b) OPoC Relationships

OPoC relationship to RNH:

- If OPoC is not the same as the RNH, OPoC must agree to OPoC status and responsibilities
    - What action is required if the OPoC is not aware of and/or does not accept the OPoC responsibilities?
- RNH must authorize OPoC for needed capabilities
    - What action is required if the RNH does not authorize the OPoC for the needed capabilities?

2 (c) OPoC Requirements

Possible enforcement issues include the following:

- OPOC lacks capabilities (see WHO)

- OPOC lacks relationships (e.g., non-accreditation)
- OPOC fails to perform

    --at all

    --in a timely fashion

AGREED: If an OPOC fails to meet its obligations in the defined response period(s), intervention is required.

SUPPORT: Registrars should intervene.

ALTERNATIVE VIEW: ICANN should intervene.

SUPPORT: If there has been a failure of the RELAY process (including a failure to forward a response from the RNH within the specified time periods), and the OPOC has not REVEALed RNH contact data, then the registrar should do so by conveying full contact details to the requester.

SUPPORT: If there is a failure of the REVEAL process, the registrar should REVEAL contact data to the requester.

ALTERNATIVE VIEW was stated under which there are no circumstances in which the full contact data of the registrant should be REVEALED simply in response to a request to the OPOC.

AGREED: ICANN would need to dedicate adequate resources to oversight of the operation of the OPOC process.

AGREED: If OPOCs were required to be accredited, the accreditation process should be robust, and loss of accreditation should be imposed on an OPOC that systematically or repeatedly failed to perform.

TO BE DISCUSSED/DETERMINED: Should ICANN be the enforcer of last resort?

TO BE DISCUSSED/DETERMINED: The following proposal regarding a registrar/registry role in carrying out the REMEDY function when the OPOC fails to do so ed but not fully discussed:

> A complainant may request that the Registrar take any of the following steps to halt illegal activity originating at the subject domain:
>
> > 1. Immediately suspend name records for the subject domain and suspend web host services.
> >
> > 2. Request the Registry to suspend website DNS (although TTL means that resolutions would still occur for 24-48 hours)
> >
> > 3. Request the Registry to lock the subject domain so that it cannot be transferred. The name should be available for resale after 90 days unless the registrant has initiated an approved dispute resolution mechanism.
>
> Any of the above steps taken to suspend resolution should not prejudice any party's ability to pursue appeals or alternate dispute resolution mechanisms.

2 (d) Access to Unpublished Whois Data

TO BE DISCUSSED/DETERMINED: Is a challenge mechanism needed for incorrect/bad faith certification of a private actor as entitled to Type I or Type II access to unpublished data?

SECTION 3 - IMPLEMENTATION DETAILS

3.1 Implementation Details Regarding Section 1(C)

1 RELAY

The OPoC must meet technical requirements for relaying messages from the Requester to the Registered Name Holder (RNH).

These requirements would include the following:

- 24x7 responsiveness
- automatic real-time forwarding of email requests from Requester to RNH
- automatic real-time forwarding of responses from RNH to Requester
- automatic copying to registrar under certain circumstances
- capability to forward requests and responses in other formats (e.g. by fax or post)

2 REVEAL

The OPoC must be capable of revealing the unpublished contact information of the RNH to the Requester in certain circumstances (*to be defined*).

The OPoC must have current contact information of the RNH, i.e. the data elements currently available publicly via Whois but unpublished under the OPoC proposal.

3 REMEDY

The OPoC has sufficient technical access and permission level to remove content or disable processes, OR authorisation from RNH to direct the registrar to take steps to resolve the problem.

How the OPoC Would Deal with Legal Requests

1. A standard format would be developed for all requests raising legal issues. One model proposed would be the eBay “Notice of Claimed Infringement.”

FOR FURTHER DISCUSSION: does a legal request include all demand letters, whether or not they relate to wrongful activity?

2. Receipt by the OPOC of a request raising legal issues would operate as a valid trigger for legal timelines and issues of sufficiency of notice. It was recognized that these issues of validity and sufficiency would ultimately be decided under national law, but it was AGREED that the RNH, not the requester, would bear the risk of failure to RELAY in a timely manner, or at all.

3. OPOC obligations upon receipt of request raising legal issues (there may be more than one obligation in a particular case):

- RELAY: It was AGREED this would be the OPOC's obligation in all cases. If requester desires relay to be withheld or delayed (e.g., for an active investigation), it should not use the OPOC process, but rather the access process developed by subgroup B.

- REVEAL: In general, this action should be taken whenever the request presents "reasonable evidence of actionable harm" (cf. the current RAA, section 3.7.7.3).

SUPPORT: The OPOC would be required to REVEAL the full RNH contact data whenever the domain name was identical or confusingly similar to a trademark or service mark in which the requester has rights (see UDRP para. 4(a)(i)).

ALTERNATIVE VIEW: REVEAL would be required only upon the filing of a UDRP case.

SUPPORT: REVEAL would be required when RELAY had failed after a specified time period.

AGREED: REMEDY would be imposed only in a to-be-defined category of "serious cases" such as phishing.

Timing of OPoC responses:

SUPPORT:

RELAY: Immediate in all cases for first leg of RELAY (OPOC to RNH). This should be automated in the case of e-mail requests.

E-mail responses from RNH to OPOC should also be forwarded to requester immediately and automatically.

If the second leg of RELAY (RNH to OPOC) is delayed, there was SUPPORT for two required actions by OPOC:

- If no RNH response is promptly received (12 hours in the case of an e-mail request that has been forwarded by e-mail), the OPOC should retry using all available means of contacting the RNH (e.g., telephone).

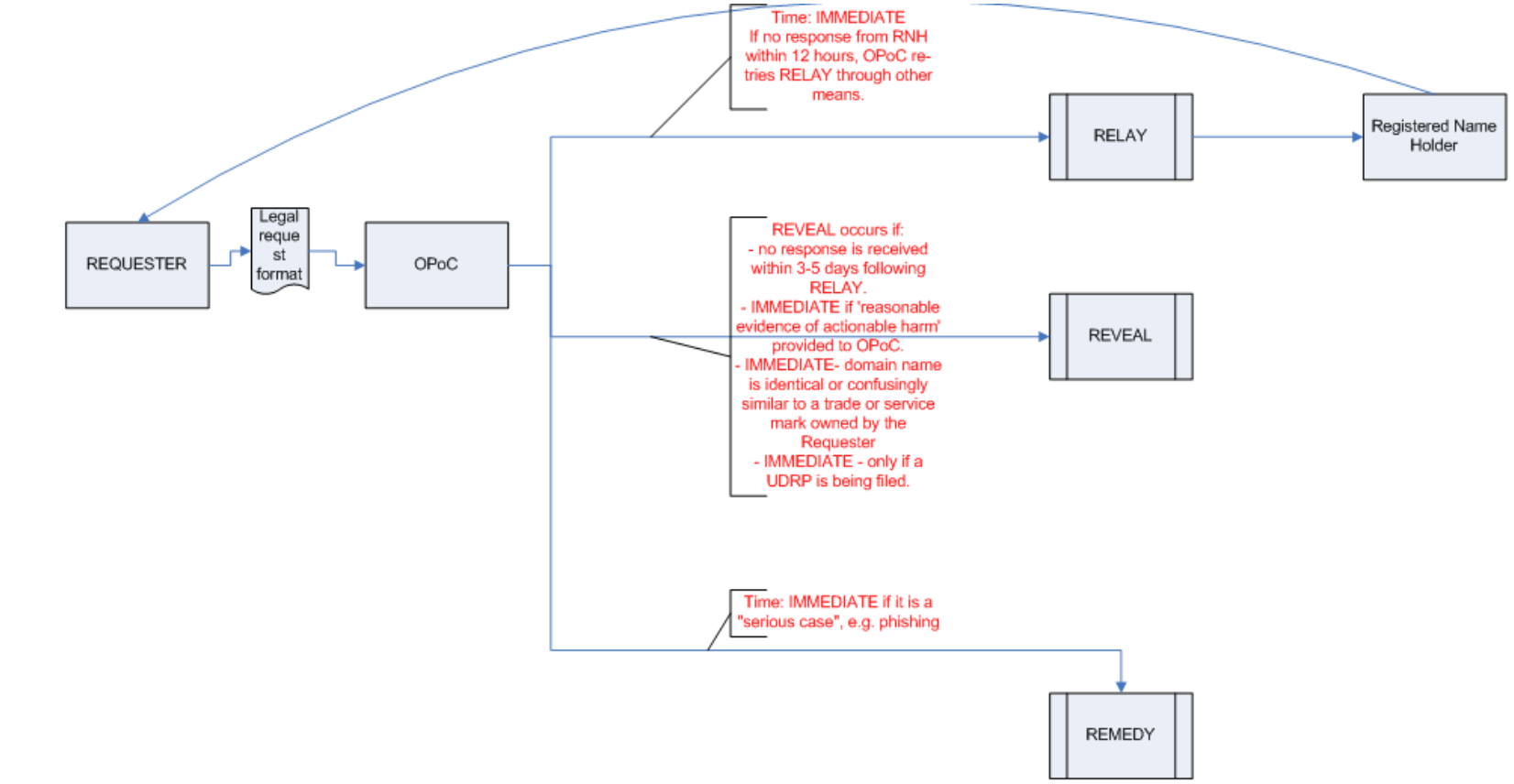
- If no RNH response is received after a longer period, the OPOC would be obligated to REVEAL the RNH contact data. A 5-day period was proposed, but others objected that this was too great a delay compared to status quo and proposed 3 days (72 hours).

REVEAL:In those cases in which the OPOC's initial obligation is to REVEAL, this should occur immediately (e.g., legal issues request that includes reasonable evidence of actionable harm). As to other cases, see bullet point above.

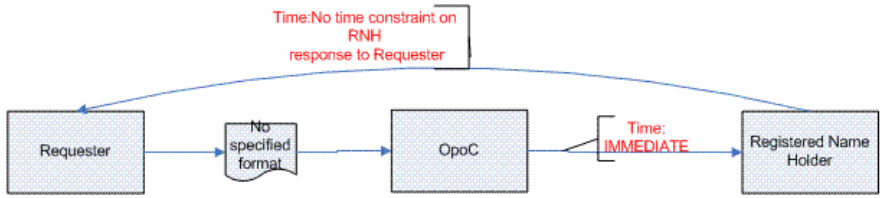
REMEDY:In the to-be-defined category of "serious cases," the REMEDY response should be immediate.

3.2 Implementation Diagrams Illustrating Treatment Of Legal And Other Requests To OPoC

The following diagrams are graphic illustrations of the mandatory OPoC attributes developed by Sub Group A:



PROCESS FOR TREATING LEGAL REQUESTS TO THE OPOC



PROCESS FOR TREATING OTHER (NON-LEGAL) REQUESTS

3.3 Implementation Issues Regarding Access To Unpublished Data:

FOR FURTHER DISCUSSION: The registries and registrars were invited on 14 June to provide information on the implementation of technical modalities for access, e.g. separate databases versus encrypted fields, the 'Blob Proposal'. What are the possible mechanisms of access?

STAFF NOTE: ICANN staff can commission initial research on technical implementation issues, e.g. at what technical 'level' (protocol/ application layer) might access mechanisms operate? What technical changes might be required? What, if any, standard-setting organisations might be affected?

ANNEX 1 – WHOIS DATA DISPLAY OPTIONS

Record	**WHOIS today**	**Retained (OPOC)**	**Full (OPOC)**
Domain ID:	x	x	x
Domain Name:	x	x	x
Created On:	x	x	x
Last Updated	x	x	x
Expiration Date:	x	x	x
Sponsoring Registrar:	x	x	x
Status*:	x	x	x
Registrant ID:	x	x	x
Registrant Name:	x	x	x
Registrant Organization:	x	x	x
Registrant Street1:	x		x
Registrant Street2:	x		x
Registrant Street3:	x		x
Registrant City:	x		x
Registrant State/Province:	x	x	x
Registrant Postal Code:	x		x
Registrant Country:	x	x	x
Registrant Phone:	x		x
Registrant Phone Ext.:	x		x
Registrant FAX:	x		x
Registrant FAX Ext.:	x		x
Registrant Email:	x		x
Natural person#		x	x
Legal person#		x	x
Proxy service operating#		x	x
OPOC*# ID:		x	x
OPOC Name:		x	x
OPOC Organization:		x	x
OPOC Street1:		x	x
OPOC Street2:		x	x

OPOC Street3:		x	x
OPOC City:		x	x
OPOC State/Province:		x	x
OPOC Postal Code:		x	x
OPOC Country:		x	x
OPOC Phone:		x	x
OPOC Phone Ext.:		x	x
OPOC FAX:		x	x
OPOC FAX Ext.:		x	x
OPOC Email:		x	x
Admin ID:	x		
Admin Name:	x		
Admin Organization:	x		
Admin Street1:	x		
Admin Street2:	x		
Admin Street3:	x		
Admin City:	x		
Admin State/Province:	x		
Admin Postal Code:	x		
Admin Country:	x		
Admin Phone:	x		
Admin Phone Ext.:	x		
Admin FAX:	x		
Admin FAX Ext.:	x		
Admin Email:	x		
Tech ID:	x		
Tech Name:	x		
Tech Organization:	x		
Tech Street1:	x		
Tech Street2:	x		
Tech Street3:	x		
Tech City:	x		
Tech State/Province:	x		
Tech Postal Code:	x		
Tech Country:	x		
Tech Phone:	x		

Tech Phone Ext.:	x		
Tech FAX:	x		
Tech FAX Ext.:	x		
Tech Email:	x		
Name Server*:	x	x	x

Key:

*	multiple entries possible
x	data collected and displayed
	data collected but not displayed
	data not collected
#	new data element conditional on new policy

The simplified OPOC assumes that the roles of the admin and tech contacts are absorbed by the OPOC. There is conditional AGREEMENT for this idea: the CONDITION is an assurance that the OPOC rights and responsibilities are meaningful so that nothing is lost in the utility of the admin and tech contacts today.

(An implementation option (if it saves cost) would be to retain the name "Admin contact" and endow the new Admin contact with the responsibilities heretofore called the OPOC.)