Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process

STATUS OF THIS DOCUMENT

This is the Initial Report on Privacy & Proxy Services Accreditation Issues, prepared by ICANN staff for submission to the GNSO Council on _____ 2014. ICANN staff will prepare a Final Report following the Working Group's review of the public comments received on this Initial Report.

SUMMARY

This report is submitted to the GNSO Council and posted for public comment as a required step in this GNSO Policy Development Process on Privacy & Proxy Services Accreditation Issues.

TABLE OF CONTENTS

1. Executive Summary

1.1 Background

On 27 June 2013, the ICANN Board approved the new 2013 Registrar Accreditation Agreement ("2013 RAA"). The 2013 RAA addressed most of the recommended high priority amendments previously proposed by the GNSO-ALAC Drafting Team in its Final Report ("RAA Final Report")[1] and law enforcement agencies ("LEA"), except for the clarification of registrar responsibilities in connection with proceedings under the Uniform Dispute Resolution Policy ("UDRP"), and issues related to privacy and proxy services, including their accreditation and reveal and relay procedures. The GNSO has since addressed the issues pertaining to a registrar's responsibilities in connection with the locking of a domain name subject to proceedings under the UDRP[2], while the UDRP itself, along with all other rights protection mechanisms, will be the subject of an Issue Report to the GNSO eighteen months after the delegation of the first generic top-level domain ("gTLD") under ICANN's New gTLD Program[3]. As such, the issues related to privacy and proxy services were identified[4] as the only remaining issues following the conclusion of the 2013 RAA negotiations that were suited for a PDP, pursuant to the October 2011 request by the ICANN Board for an Issue Report when initiating negotiations for the 2013 RAA with the gTLD Registrars Stakeholder Group[5].

On 31 October 2013, the GNSO Council initiated a Policy Development Process and chartered the Privacy & Proxy Services Accreditation Issues ("PPSAI") Working Group. A Call for Volunteers to the

[1] See http://gnso.icann.org/issues/raa/raa-improvements-proposal-final-report-18oct10-en.pdf.

[2] See http://gnso.icann.org/en/group-activities/active/locking-domain-name.

[3] See http://gnso.icann.org/en/council/resolutions#201112.

[4] See the Report on the Conclusion of the 2013 RAA Negotiations, prepared by ICANN staff in September 2013: http://gnso.icann.org/en/issues/raa/negotiations-conclusion-16sep13-en.pdf.

[5] See https://www.icann.org/resources/board-material/resolutions-2011-10-28-en#7.

Working Group ("WG") was issued on 6 November 2013, and the WG held its first meeting on 3 December 2013[6].

1.2 Deliberations of the Working Group

The PPSAI Working Group started its work on 3 December 2013. The WG decided to conduct its deliberations primarily through weekly conference calls, in addition to discussions on its mailing list and scheduled meetings during ICANN Public Meetings. Section 5 provides an overview of the deliberations of the Working Group conducted by conference call as well as through e-mail threads and at ICANN Public Meetings.

The WG agreed early on to group the twenty-one questions outlined in its Charter into seven categories of related questions. For each Charter question, the WG used a uniform template that contained relevant background information to that question, community input received, WG member survey responses and other relevant material to inform its discussions and development of the preliminary conclusions presented for public comment in this Initial Report.

The WG's findings and initial recommendations for each of these Charter questions can be found in full in Section 7 of this Initial Report. They are also summarized in Section 1.3 that follows.

1.3 WG Preliminary Recommendations

The WG was chartered to provide the GNSO Council with "policy recommendations regarding the issues identified during the 2013 RAA negotiations, including recommendations made by law enforcement and GNSO working groups, that were not addressed during the 2013 RAA negotiations and otherwise suited for a PDP; specifically, issues relating to the accreditation of Privacy & Proxy Services". Following its analysis of each of the questions outlined in its Charter related to this task, the WG has arrived at a set of preliminary conclusions, although in several instances the WG has not yet finalized an agreed position on particular issues. These instances are clearly marked as such in this Initial Report. For at least one group of Charter questions, the WG is currently divided with a majority and minority view; this is also specifically indicated in the text of this Initial Report. A formal consensus call on all the Charter

[6] For background information on the formation and deliberations of the WG, see the WG wiki workspace at https://community.icann.org/x/9iCfAg.

questions will take place once the WG finalizes all its recommendations following its review of public comments received.

The WG believes that its final recommendations, if approved by the GNSO Council and the ICANN Board, will substantially improve the current environment, where there is presently no accreditation scheme for privacy and proxy services and no community-developed or accepted set of baseline or best practices for such services. It hopes that its recommendations will provide a sound basis for the development and implementation of an accreditation framework by ICANN, as part of ICANN's on-going efforts to improve the WHOIS system, including implementing recommendations made by the WHOIS Policy Review Team[7].

The following sub-sections provide a summary of the WG's preliminary conclusions as follows[8]:

- Section 1.3.1 contains all the WG's preliminarily-agreed recommendations;
- Section 1.3.2 contains those of the WG's deliberations and preliminary conclusions that have yet to be finalized and for which public comments are considered particularly helpful; and
- Section 1.3.3 contains the WG's majority and minority view on specific topics, and for which specific public comments are also considered helpful in facilitating the WG's finalization of its recommendations.

The full text of all of the WG's preliminary conclusions, including any supplemental notes, are set out in detail in Section 7.

1.3.1 Summary of the WG's agreed preliminary conclusions

The WG has reached preliminary agreement on the following recommendations:

1. Privacy and proxy services ~~could potentially~~ can be treated the same way for the purpose of the accreditation process.

[7] See ICANN's Action Plan for the WHOIS Policy Review Team Final Report (November 2012): https://www.icann.org/en/system/files/files/implementation-action-08nov12-en.pdf.

[8] Where specific language, options or recommendations are still under consideration by the WG, these have been indicated by the use of square brackets around the relevant text.

2. Domain name registrations involving privacy/proxy service providers should be clearly labelled as such in WHOIS[9].

3. Proxy and privacy customer data is to be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Specification of the 2013 RAA. In the cases where, for P/P providers Affiliated with a registrar (as defined by the 2013 RAA), validation and verification of the P/P customer data was carried out by the registrar, re-verification by the P/P service of the same, identical, information should not be required.

4. All rights, responsibilities and obligations for registrants as well as privacy/proxy providers need to be clearly communicated in the privacy/proxy registration agreement, including any specific requirements applying to transfers and renewals (note that further details as to minimum requirements for rights, responsibilities and obligations may need to be developed).

5. The following should be mandatory requirements of a P/P Accreditation Program[10]:
   - All P/P services must relay to their customers any notices required under the RAA or an ICANN Consensus Policy.
   - All P/P service registration agreements must state the customer's rights and responsibilities and the P/P service's obligations in managing those rights and responsibilities. Specifically, all P/P services must disclose to their customers the conditions under which the service may be terminated in the event of a transfer of the domain name, and how requests for transfers of a domain name are handled.
   - In addition to the above, the WG recommends that certain other requirements in relation to "reveal" requests and practices in the event of de-accreditation be made mandatory

[9] ~~The~~ While this may be possible with existing fields, the WG ~~acknowledges that implementing this recommendation may require analysis of the possible implications of adding another field to WHOIS.~~has also explored the idea that the label might also be implemented by adding another field to WHOIS, and the questions that this may raise.

[10] See also Recommendation #17 in this Section 1.3.1 concerning mandatory provisions in a provider's terms of service, and generally Section 7, below.

in the terms of service offered by P/P services. These are summarized in Recommendations 17 & 18 of this Section 1.3.1 (below) and detailed in Section 7 of this Initial Report.

6. In addition, the WG recommends the following as best practices for accredited P/P providers[11]:
   - P/P services should facilitate and not ~~hinder~~ obstruct the transfer, renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the ERRP and transfers to another P/P service.
   - P/P services should use commercially reasonable efforts to avoid the need to disclose underlying customer data in the process of renewing, transferring or restoring a domain name.

7. The status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether proxy/privacy services are available to the registrant. Fundamentally, P/P services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals. Further, privacy/proxy registrations should not be limited to private individuals who use their domains for non-commercial purposes[12].

8. ICANN should publish and maintain a publicly accessible list of all accredited P/P providers, with all appropriate contact information. Registrars should provide a web link to P/P services run by them or their Affiliates, and P/P providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program[13].

[11] The WG recognizes that implementation of these recommendations may involve the development of new procedures.

[12] Note that while the WG agreed ~~on there being~~ that there is no reason to distinguish between commercial and non-commercial registrants simply because of their organizational/entity status, ~~there is not yet a consensus view~~it has not reached consensus as to whether the use of P/P services for certain types of commercial activity associated with a domain name should ~~not be permitted to use P/P services~~be barred (see Sections 1.3.3 and 7, below).

[13] The WG discussed, but has not yet reached consensus on, the possibility of requiring a registrar to also declare its Affiliation (if any) with a P/P provider.

9. A "designated" rather than a "dedicated" point of contact will be sufficient for abuse reporting purposes, since the primary concern is to have one contact point that third parties can go to and expect a response from.

10. P/P providers should be fully contactable (but note that the WG has yet to reach agreement on whether adopting Section 2.3 (from the 2013 RAA Interim Privacy & Proxy Specification) will be sufficient in this regard).

11. Requirements relating to the forms of alleged malicious conduct to be covered by the designated published point of contact at an ICANN-accredited privacy/proxy service provider should include a list of the forms of malicious conduct to be covered. These requirements should allow for enough flexibility to accommodate new types of malicious conduct. By way of example, Section 3 of the Public Interest Commitments (PIC) Specification[14] in the New gTLD Registry Agreement or Safeguard 2, Annex 1 of the GAC's Beijing Communique[15] could serve as ~~examples for how this could be achieved~~starting points for developing such a list.

12. A standardized form for information requests and reports should be developed, to also include space for free form text[16]. It was also suggested that providers should have the ability to "categorize" reports received, in order to facilitate responsiveness.

13. Regarding Relaying (Forwarding) of Electronic Communications[17]:

---

[14] See http://newgtlds.icann.org/en/applicants/agb/agreement-approved-20nov13-en.pdf; Section 3 provides that "Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."

[15] See https://www.icann.org/en/system/files/correspondence/gac-to-board-11apr13-en.pdf; Safeguard 2, Annex 1 provides that ""Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law."

[16] The WG discussed but did not finalize the minimum elements that should be included in such a form.

[17] The WG agrees that emails, web forms and automated telephone calls would be considered "electronic communications" whereas human-operated faxes and non-automated telephone calls would not. The WG

- All communications required by the RAA and ICANN Consensus Policies must be forwarded
- For all other electronic communications, providers may elect one of the following two options:
    i. Option #1: Forward all electronic requests received (including emails and via web forms), but the provider may implement commercially reasonable safeguards (including CAPTCHA) to filter out spam and other forms of abusive communications, or
    ii. Option #2: Forward all electronic requests (including those received via emails and web forms) received from law enforcement authorities and third parties containing allegations of domain name abuse (i.e. illegal activity)
- In all cases, providers must publish and maintain a mechanism (e.g. designated email point of contact) for requestors to contact to follow up on or escalate their original requests.

14. Regarding Further Provider Actions When There Is A Persistent Delivery Failure of Electronic Communications

- All third party electronic requests alleging abuse by a P/P customer will be promptly forwarded to the customer. A requestor will be promptly notified of a persistent failure of delivery[18] that a provider becomes aware of.
- The WG considers that a "persistent delivery failure" will have occurred when an electronic communications system abandons or otherwise stops attempting to deliver an electronic communication to a customer after [a certain number of] repeated or duplicate delivery attempts within [a reasonable period of time][19]. The WG emphasizes that such persistent delivery failure, in and of itself, is not sufficient to trigger further provider obligation or action under this Category E unless the provider also becomes aware of the persistent delivery failure.

---

recommends that implementation of the concept of "electronic communications" be sufficiently flexible to accommodate future technological developments.

[18] The WG notes that failure of "delivery" of a communication is not to be equated with the failure of a customer to "respond" to a request, notification or other type of communication.

[19] Although the WG has agreed on this concept in principle, it welcomes community input on the specific timeframes and number of attempts that would qualify as a persistent delivery failure.

- A persistent delivery failure to a customer as described herein will trigger the provider's obligation to perform a verification/re-verification (as applicable) of the customer's email address(es), in accordance with the WG's recommendation under Category B, Question 2.
- However, these recommendations shall not preclude a provider from taking any additional action in the event of a persistent delivery failure of electronic communications to a customer, in accordance with its published terms of service.

15. Agreed Definitions relevant to "Reveal" which the WG recommends be used uniformly, including generally in relation to WHOIS and beyond privacy and proxy service issues:
    - "Publication" means the reveal of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details in the WHOIS system.
    - "Disclosure" means the reveal of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details to a third party requestor without Publication in the WHOIS system.
    - The term "person" as used in these definitions is understood to include natural and legal persons, as well as organizations and entities.
    - "Law enforcement authority" means law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the P/P service provider is established or maintains a physical office.

16. Regarding relay and reveal, the WG agreed that none of its recommendations should be read as being intended to alter (or mandate the alteration of) the prevailing practice among providers to review requests manually or to facilitate direct resolution of an issue between a requestor and a customer. It also notes that disclosure of at least some contact details of the customer may in some cases be required in order to facilitate such direct resolution.

17. Accredited providers should indicate the following elements clearly in their terms of service:
    - When referring to Publication requests (and their consequences) and when to Disclosure requests (and their consequences). The WG further recommends that accredited providers

expressly include a provision in their terms of service explaining the meaning and consequences of Publication

- The specific grounds upon which a customer's details may be Disclosed or Published or service suspended or terminated
- Whether or not a customer: (1) will be notified when a provider receives a Publication or Disclosure request from a third party; and (2) in the case of Publication, whether the customer may opt to cancel its domain registration prior to and in lieu of Publication
- That a requestor will be notified in a timely manner of the provider's decision: (1) to notify its customer of the request; and (2) whether or not the provider agrees to comply with the request to Disclose or Publish. This should also be clearly indicated in all Disclosure or Publication related materials.

18. ICANN's Accreditation Program must include a requirement for all accredited providers to include on their websites, and in all Publication or Disclosure-related policies and documents, a link to a [standardized] Request Form or an equivalent list of specific criteria that the provider requires in order to comply with such requests.

19. Regarding de-accreditation of a P/P provider:
    - P/P customers should be notified prior to de-accreditation of a provider, to enable them to make alternative arrangements. One possible time in which to do so might be when Compliance sends breach notices to the provider, as customers would then be put on notice (as is done for registrar de-accreditation).
    - Other P/P providers should also be notified, to enable interested providers to indicate if they wish to become the gaining P/P provider (as is done for registrar de-accreditation)
    - All notification(s) are to be published on the ICANN website (as is done for registrar de-accreditation)
    - A de-accredited P/P provider should have the opportunity to find a gaining provider to work with (as sometimes occurs with registrar de-accreditation)
    - A "graduated response" approach to de-accreditation should be explored, i.e. a set series of breach notices (e.g. up to three) with escalating sanctions, with the final recourse being de-accreditation

- [A customer should be able to choose its new P/P provider]
- The next review of the IRTP should include an analysis of the impact on P/P customers, to ensure that adequate safeguards are in place as regards P/P protection when domain names are transferred pursuant to an IRTP process

1.3.2 Summary of topics on which the WG has yet to finalize preliminary conclusions

The following are the questions/preliminary conclusions on which the WG has yet to reach agreement, and for which it specifically invites community input.

On Contactability and Responsiveness of Accredited P/P Providers:

- What should be the standard for maintaining a designated point of contact – "reasonable and prompt" (per the TEAC) or other?
- What should be required of P/P providers in terms of level of responsiveness – "reasonable and prompt" (per the 2013 RAA) or other?
- Should the standard for provider contactability be the same as that under Section 2.3 of the 2013 RAA?

On Escalation of Relay Requests:

While the WG reached preliminary agreement on a provider's obligation to act in the event it becomes aware of a persistent delivery failure, the WG has yet to agree on obligatory next steps for a provider regarding escalation by a requestor. The following is the current language under consideration by the WG, with the options included in square brackets:

> *"As part of an escalation process, and when the above-mentioned requirements concerning a persistent delivery failure of an electronic communication have been met, the provider [should] [must] upon request forward a further form of notice to its customer. A provider should have the discretion to select the most appropriate means of forwarding such a request [and to charge a reasonable fee on a cost-recovery basis]. [Any such reasonable fee is to be borne by the customer and not the requestor]. A provider shall have the right to impose reasonable limits on the number of such requests made by the same requestor."*

- What should be the minimum mandatory requirements for escalation of relay requests in the event of a persistent delivery failure of an electronic communication?

On Disclosure and Publication in relation to Requests by LEA and other Third Parties:

- Should there be uniform minimum standards for accredited P/P providers to apply in determining when to Disclose or Publish, or in verifying a requestor's identity?
- Should it be mandatory for accredited P/P providers to comply with express LEA requests not to notify a customer? Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity? What (if any) should the remedies be for unwarranted Publication?
- Should it be mandatory for accredited P/P providers to comply with express requests for Disclosure for the purpose of sending cease and desist letters or notices of formal legal proceedings against the customer? Should customer notification in such cases be mandatory?

In addition, the WG is considering the following language for requests by intellectual property rights owners or their representatives:

- *Provider to notify customer when it receives a Disclosure request relating to an "IP complaint stated with great specificity, including the identity of the IP rights holder and complainant, the right(s) involved, and the nature of the infringing activity"*[20].
- *There should be a period (of X number of days?) for the customer to take action in response to the notification. This may take the form of a direct response to the requestor, a request to cancel its domain name registration, file with a court or other actions.*
- *Provider [may] [shall] proceed to Disclose if customer does not take responsive action within the specified time frame (but how would provider know that customer has done so? Perhaps require that customer acknowledge receipt of the notification and its intention to take action?)*
- *Any such Disclosure should be subject to reasonable limitations on the use of such Disclosed information.*

[20] The quoted language reproduces verbatim language suggested by a WG member.

On the Consequences of Termination of a Customer's P/P Service:

- Are the WG's minimum recommendations in Category F regarding mandatory provisions to be included in a provider's terms of service sufficient to facilitate protection of P/P customers in the event of Publication of a customer's details in WHOIS as a result of termination of P/P service to that customer (including where this was due to the customer's breach of the terms of service)?

1.3.3 Summary of topics on which there is both a majority and minority view within the WG

Although the WG agreed that the mere fact that a domain name is registered by a commercial entity or by anyone conducting commercial activity should not preclude the use of P/P services[21], there was disagreement over whether domain names that are actively used for commercial transactions (e.g. the sale or exchange of goods or services) should be prohibited from using P/P services. While a majority did not believe such a prohibition is necessary or practical, a minority believed that registrants of such domain names should not be able to use or continue using proxy or privacy services. In the minority view, it was noted that businesses in the "offline world" are often required to register with relevant authorities as well as disclose details about their identities and locations. These WG members expressed the view that it is both necessary and practical to distinguish between domains used for a commercial purpose (irrespective of whether the registrant is actually registered as a commercial entity anywhere) and those domains (which may be operated by commercial entity) that are used for a non-commercial purpose.

The WG chairs suggested that such domains might be more usefully termed "transactional" rather than more generally "commercial" domains. They developed the following suggested definition and potential recommendation to describe the minority view regarding these transactional domains: *"domains used for online financial transactions for commercial purpose should be ineligible for privacy and proxy registrations."*

[21] The WG notes that the WHOIS RT had specifically acknowledged that privacy and proxy services can be and are used to address legitimate interests, both commercial and non-commercial.

The community is invited to provide input on the following questions:

- Should the majority or minority view of the WG be adopted?
- Will it be useful to adopt a definition of "commercial" or "transactional" (and if so, should this be that suggested in the text or some other)?
- Will it be necessary to make a distinction in the WHOIS data fields to be displayed as a result?

1.4 Community Input

The WG reached out to all ICANN Supporting Organizations and Advisory Committees as well as GNSO Stakeholder Groups and Constituencies with a request for input (see Annexes B and C) at the start of its deliberations. All responses received were reviewed by the WG and incorporated into its templates for each of its Charter questions.

The WG also reviewed the responses to a February 2014 privacy and proxy provider questionnaire[22] developed by the Expert Working Group on gTLD Data Directory Services ("EWG") as well as other relevant background material, including the recommendations from the EWG and the WHOIS Policy Review Team[23].

1.5 Conclusions and Next Steps

The Working Group aims to complete this section of the report following its review of public comments received on this Initial Report.

[22] See https://community.icann.org/download/attachments/45744698/EWG%20PP%20PROVIDER%20QUESTIONNAIRE%20SUMMARY%2014%20March%202014.pdf?version=1&modificationDate=1395362247000&api=v2.
[23] These can be accessed on the WG wiki at https://community.icann.org/x/XSWfAg.

2. Objective and Next Steps

This Initial Report on Privacy & Proxy Services Accreditation Issues is prepared as required by the GNSO Policy Development Process as stated in the ICANN Bylaws, Annex A (see http://www.icann.org/general/bylaws.htm#AnnexA). The Initial Report will be posted for public comment for at least 40 days. The comments received will be analyzed by the WG as part of its development of a Final Report to be considered by the GNSO Council for further action.

3. Background

3.1 Process Background

- At the ICANN Meeting in Dakar in October 2011 the ICANN Board adopted a Resolution regarding amendments to the Registrar Accreditation Agreement (the "Dakar RAA Resolution").
- The Dakar RAA Resolution directed that negotiations on amending the 2009 RAA be commenced immediately, and clarified that the subject matter of the negotiations was to include the recommendations made by LEA, those made in the RAA Final Report, as well as other topics that would advance the twin goals of achieving registrant protection and domain name system ("DNS") stability. This resolution further requested the creation of an Issue Report to undertake a GNSO PDP as quickly as possible, to address any remaining items not covered by the negotiations and otherwise suited for a PDP.
- In response to the Dakar RAA Resolution, ICANN published the Final GNSO Issue Report on 6 March 2012. In this Final Issue Report, ICANN staff recommended that the GNSO Council commence a PDP on the RAA amendments upon either: (i) receipt of a report that the RAA negotiations have concluded, or that any of the 24 Proposed Amendment Topics identified in the Final Issue Report are no longer actively being negotiated, or (ii) a Board instruction to proceed with a PDP on any or all of the Proposed Amendment Topics identified in the Final Issue Report.
- On 27 June 2013, the ICANN Board approved the new 2013 RAA.
- On 16 September 2013, ICANN staff published a report for the GNSO Council on the conclusion of the 2013 RAA negotiations, recommending that the GNSO Council proceed to commence the Board-requested PDP, on remaining issues not addressed by the 2013 RAA and otherwise suited to a PDP, i.e. issues pertaining to privacy and proxy services.
- On 31 October 2013 the GNSO Council approved the initiation of the PDP and the Charter for the Privacy & Proxy Services Accreditation Issues Working Group ("PPSAI WG").

3.2 Issue Background

3.2.1 The Outcome of the 2013 RAA Negotiations

The RAA Final Report includes a number of High Priority and Medium Priority topics. The 2013 RAA negotiations addressed most of the High and Medium Priority topics as well as recommendations received from LEA. As noted in the Staff Report on the Conclusion of the 2013 RAA Negotiations, out of these topics and recommendations, only two remained after the completed negotiations as not addressed adequately: (1) clarification of registrar responsibilities in connection with proceedings under the existing UDRP; and 2) privacy and proxy services – including accreditation and reveal/relay procedures.

The UDRP-related issue has since been addressed in the recommendations that were adopted in August 2013 by the GNSO Council for the locking of a domain name subject to UDRP proceedings; these were in turn approved by the ICANN Board in September 2013.

With regard to privacy and proxy services, the 2013 RAA provides an interim specification[24] that will be in place until the earlier either of 1 January 2017, or until any PDP recommendations are developed by the GNSO and adopted by the ICANN Board. The specification includes a limited set of minimum requirements that ICANN-accredited Registrars, their Affiliates and Resellers have to comply with. These minimum requirements include: (1) disclosure of key service terms; (2) publication of infringement/abuse point of contact; (3) publication of business contact information; and (4) escrow of customer data.

During the 2013 RAA negotiations, ICANN and the Registrars' negotiating team had agreed that a number of interim protections would be in place for proxy and privacy services offered through Registrars or their Affiliates. These interim protections require that information be made available on matters such as abuse reporting processes and the circumstances under which a provider will relay third party communications to a privacy or proxy customer, terminate a customer's service, and publish a customer's details in WHOIS. While these are not necessarily comprehensive in terms of the terms and

[24] See https://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#privacy-proxy.

protections that can be put in place for accredited proxy and privacy providers, these interim protections were intended to provide a more responsible marketplace until a formal accreditation program is developed by ICANN.

Other relevant information, materials and prior work that were taken into account by the GNSO Council in chartering the PPSAI WG, and that were reviewed or noted by the WG during its deliberations, are highlighted below[25].

3.2.2 Related Work by the GNSO and ICANN Community

The ICANN community, including the GAC and the GNSO, had previously raised a number of issues and concerns regarding privacy and proxy services. Besides the work of the GNSO and At Large communities on the RAA Final Report, the WHOIS-related studies approved by the GNSO Council in between 2009 and 2011 also formed part of the background material for the PPSAI WG. These studies included one on Privacy & Proxy Service Abuse that was conducted by the National Physical Laboratory ("NPL") in the United Kingdom. NPL's final results were published in March 2014. The GNSO Council had also approved a Pre-Feasibility Survey on Relay and Reveal Procedures, conducted by the Interisle Consulting Group, who published their findings in August 2012.

The GAC had previously issued a set of Principles regarding gTLD WHOIS Services in 2007[26], and had also proposed a number of topic and study areas to the GNSO in 2008. In addition, several GNSO study groups had worked on study proposals relating to WHOIS services, and developed key definitions (including for privacy and proxy services) that were used to frame the GNSO's WHOIS studies.

3.2.3 Recommendations from the WHOIS Policy Review Team

[25] These were summarized in the form of an Issue Chart in the Staff Report on the Conclusion of the 2013 RAA Negotiations, and formed the basis for the PPSAI WG Charter that was approved by the GNSO Council in October 2013.

[26] See https://gacweb.icann.org/download/.../WHOIS_principles.pdf.

The WHOIS Policy Review Team ("WHOIS RT"), constituted as part of ICANN's Affirmation of Commitments with the United States Government, published its Final Report[27] in May 2012. The Final Report had highlighted the lack of clear and consistent rules regarding privacy and proxy services, resulting in unpredictable outcomes for stakeholders. The WHOIS RT noted that appropriate regulation and oversight over such services would address stakeholder needs and concerns, and recommended that ICANN consider an accreditation system, with the goal of providing "clear, consistent and enforceable requirements for the operation of these services consistent with national laws, and to strike an appropriate balance between stakeholders with competing but legitimate interests. At a minimum, this would include privacy, data protection, law enforcement, the industry around law enforcement and the human rights community."

The WHOIS RT also recommended that ICANN consider "a mix of incentives and graduated sanctions to encourage privacy/proxy service providers to become accredited, and to ensure that registrars do not knowingly accept registrations from unaccredited providers". For example, "ICANN could develop a graduated and enforceable series of penalties for proxy/privacy service providers who violate the requirements, with a clear path to de-accreditation for repeat, serial or otherwise serious breaches."

The WHOIS RT went on to list several specific possible objectives and recommendations for consideration, as follows:

- Clearly labeling WHOIS entries to indicate that registrations have been made by a privacy or proxy service;
- Providing full WHOIS contact details for the privacy/proxy service provider, which are contactable and responsive;
- Adopting agreed standardized relay and reveal processes and timeframes; (these should be clearly published, and pro-actively advised to potential users of these services so they can make informed choices based on their individual circumstances);
- Registrars should disclose their relationship with any proxy/privacy service provider;
- Maintaining dedicated abuse points of contact for each provider;
- Conducting periodic due diligence checks on customer contact information;

[27] See https://www.icann.org/en/about/aoc-review/whois/final-report-11may12-en.

- Maintaining the privacy and integrity of registrations in the event that major problems arise with a privacy/proxy provider; and
- Providing clear and unambiguous guidance on the rights and responsibilities of registered name holders, and how those should be managed in the privacy/proxy environment.

3.2.4 Recommendations of the EWG on gTLD Data Directory Services

The EWG had been formed in December 2012 as a first step toward fulfilling the ICANN Board's directive to assist in redefining the purpose and provision of gTLD registration data, and to provide a possible foundation for the GNSO to develop a new policy for gTLD directory services. In requesting that ICANN staff address the topic, the Board had also requested an Issue Report, kicking off a Board-mandated PDP, to address the purpose of collecting, maintaining and making available gTLD registration data as well as related issues pertaining to data accuracy and access.

The EWG published its Final Report in June 2014, which included certain recommendations relating to privacy and proxy services[28]. It noted the current lack of standard processes and the prior work that had been done by the GNSO and ICANN community, and highlighted certain common needs to be addressed:

- Relaying communications to a privacy or proxy service customer – provided by many but not all providers, this is often done by auto-forwarding email sent to the customer's admin/tech contact email address
- Revealing the identity and direct contact details for a proxy customer in response to a third party complaint – here, processes, documentation, responsiveness, and actions taken vary and often depend on established relationships between requestors and providers
- Unmasking the identity of the underlying customer and publishing his/her name and contact details in WHOIS
- Requestors often look to the Registrar (which may or may not be affiliated with the provider) for escalation or assistance when they fail to contact the underlying customer or when there is no resolution from the provider

[28] See Section VII of the EWG Final Report: https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf.

The EWG recommended accrediting privacy and proxy service providers in general, and offered the following additional specific recommendations[29]:

- Entities and natural persons may register domain names using accredited privacy services that do not disclose the Registrant's contact details except in defined circumstances (e.g., terms of service violation or in response to a subpoena) as well as accredited proxy services that register domain names on behalf of the customer
- ICANN must require specific terms to be included in the terms of service, which must include requiring the service provider to endeavor to provide notice in cases of expedited take-downs
- Accredited services must provide the Registrar with accurate and reliable contact details for all mandatory Purpose-Based Contacts[30], in order to reach the provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Registrant
- Accredited services must be obligated to relay emails received by the Registrant's forwarding email address
- Accredited proxy service providers must provide the Registrar with their own Registrant name and contact details, including a unique forwarding email address to contact the entity authorized to register the domain name on behalf of the customer
- As the registered name holder, accredited proxy service providers must assume all the usual Registrant responsibilities for that domain name, including provision of accurate and reliable mandatory Purpose-Based Contacts and other registration data
- Accredited Proxy services must be obligated to respond to reveal requests in a timely manner

[29] See Recommended Principles 138-149 from Section VII of the EWG Final Report as well as Annex H.
[30] This concept was developed by the EWG as part of its proposed Registration Directory Service ("RDS") and is further described in their report.

4. Approach taken by the Working Group

4.1 Working Methodology

The PPSAI WG began its deliberations on 3 December 2013. It decided to continue its work primarily through weekly conference calls, in addition to e-mail exchanges on its mailing list, with further discussions taking place at ICANN Public Meetings when scheduled. All the WG's meetings are documented on its wiki workspace, including its mailing list, draft documents, background materials and input received from ICANN's SO/ACs and the GNSO's Stakeholder Groups and Constituencies.

The WG also prepared a Work Plan, which was reviewed on a regular basis. In order to facilitate its work, the WG decided to use a template to tabulate all input received in response to its request for Constituency and Stakeholder Group statements (see Annex B). This template was also used to record input from other ICANN Supporting Organizations and Advisory Committees, as well as individual WG members' responses (either on their own behalf or as representatives of their respective groups) to a survey that was conducted among the WG concerning each of the WG's Charter questions.

The WG scheduled community sessions at each ICANN Public Meeting that took place after its formation, at which it presented its preliminary findings and/or conclusions to the broader ICANN community for discussion and feedback. The WG was also selected by the GNSO Council to be the first WG to participate in the GNSO Council's pilot project to facilitate effective WG consensus-building in FY2015. This took the form of a full-day face-to-face (in-person as well as remotely) meeting at the ICANN Public Meeting in Los Angeles in October 2014, facilitated by a community facilitator with expertise on the topic.

4.2 Members of the Working Group

The members of the PPSAI WG are:

NCSG	Affiliation*	Attended**
Amr Elsadr	NCUC	19
David Cake		20
Maria Farrell++	NCUC	13
Marie-Laure Lemineur	NPOC	11
Roy Balleste	NCUC	17
Stephanie Perrin	NCUC	26
Wendy Seltzer	NCUC	1
Howard Fellman	NCUC	
Kathy Kleiman		40

CSG		
Adamou Nacer	ISPCP	1
Alex Deacon	IPC	32
Hector Ariel Manoff	IPC	1
Brian Winterfeldt	IPC	3
Keith Kupferschmid	IPC	15
Kiran Malancharuvil	IPC	22
Kristina Rosette	IPC	31
Steve Metalitz	IPC	33
Osvaldo Novoa	ISPCP	28
Philip Marano	IPC	35
Todd Williams	IPC	30
Victoria Scheckler	IPC	12
Griffin Barnett	IPC	40
Valeriya Sherman	IPC	40
David Hughes	IPC	8
Paul McGrady	IPC	27
Jim Bikoff	IPC	35
David Heasley	IPC	37
Don Moody	IPC	10

Emily Emanual	BC	4
Michael Adeyeye	BC	
Justin Macy	BC	40
John Horton	BC	9
Libby Baney	BC	25
Michael Shoukry	BC	1
Christain Dawson	ISPCP	20
Laura Jedeed	BC	9
Katherine McGowan++	BC	
Susan Kawaguchi	BC	21
Chris Chaplow	BC	1
Phil Corwin	BC	12

RrSG

Ben Anderson	4
Jeffrey Eckhaus	
Gordon Dick	5
Graeme Bunton	42
Tatiana Khramtsova	33
James Bladel	36
Luc Seufer	33
Matt Serlin	2
Michele Neylon	33
Nicolas Steinbach	6
Rob Villeneuve	
Tobias Sattler	15
Susan Prosser	21
Tim Ruiz	22
Volker Greimann	37
Theo Geurts	12
Sarah Wyld	33

Darcy Southwell		34
Billy Watnpaugh		3
Jennifer Standiford		11
Chris Pelling		29
Bob Wiegand		
Lindsay Hamilton-Reid		7
Ivens Oliveira Porto		
RySG		
Don Blumenthal		39
Michael Palage		5
Statton Hammock		4
Bret Fausett		1
At Large/ALAC		
Bob Bruen		
Carlton Samuels		25
Holly Raiche		26
Individuals		
Eric Brunner-Williams		1
Dan Burke++		3
Frank Michlick		24
William Lin		
Other		
Gema Maria Campillos	GAC	8
Richard Leaning		2

The Statements of Interest of the WG members can be found at https://community.icann.org/x/c4Lg.

The attendance records can be found at https://community.icann.org/x/xrbhAg. The email archives can be found at http://mm.icann.org/pipermail/gnso-ppsai-pdp-wg/.

* The following are the ICANN SO/ACs and GNSO Stakeholder Groups and Constituencies for which WG members provided affiliations:

RrSG – Registrar Stakeholder Group
RySG – Registry Stakeholder Group
CBUC – Commercial and Business Users Constituency
NCUC – Non-Commercial Users Constituency
IPC – Intellectual Property Constituency
ISPCP – Internet Service and Connection Providers Constituency
NPOC – Not-for-Profit Organizations Constituency
GAC – Governmental Advisory Committee

** This list was accurate as of 15 December 2014 and will be updated for publication. Note that some members joined the WG only after it began meeting in December 2013, and several WG members have also since left (these are indicated with ++ against their names).

5. Deliberations of the Working Group

This Section provides an overview of the deliberations of the WG. The points outlined below are meant to provide the reader with relevant background information on the WG's deliberations and processes, and should not be read as either final recommendations or as representing the entirety of the deliberations of the WG. The WG will not finalize its recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report.

5.1 Initial Fact-Finding and Research

Per its Charter, the WG was tasked to review a list of topics and questions, as part of its work to develop policy recommendations relating to the accreditation of privacy and proxy services. These topics and questions were derived in large part from the prior work done by the ICANN community, as noted in Section 3 above.

The WG grouped all its Charter questions into seven specific categories, as follows: Main Issues; Maintenance of Privacy/Proxy Services; Registration of Privacy/Proxy Services; Contact Point to be Provided by Privacy/Proxy Services; Relay of Complaints to a Privacy/Proxy Customer; Reveal of the Identity or Contact Details of a Privacy/Proxy Customer; and Termination of Privacy/Proxy Services and De-Accreditation of Privacy/Proxy Service Providers[31]. Each category and the Charter questions grouped within it are listed in further detail below.

In order to obtain as much information as possible at the outset of the process, a survey was conducted amongst the WG membership. In addition, the WG requested input from GNSO Stakeholder Groups and Constituencies, as well as other ICANN Supporting Organizations and Advisory Committees (see Annexes B & C and section 6 for further details).

[31] See the WG's Final Grouping of Charter Questions (as of 23 February 2014): https://community.icann.org/download/attachments/47256202/Clean%20PPSAI-Charter-QuestionsGrouping-13%20Feb%202014.doc?version=1&modificationDate=1397484425000&api=v2.

5.2 Main Issues (Charter Questions Grouping Category A)

The following Charter questions were grouped into this Category A, as the WG believed these to be of a more general nature. Other, more specific questions were consequently grouped into more focused categories (B through G).

1. What, if any, are the types of Standard Service Practices that should be adopted and published by ICANN-accredited privacy/proxy service providers?

2. Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?

3. What are the effects of the privacy and proxy service specification contained in the 2013 RAA? Have these new requirements improved WHOIS quality, registrant contactability and service usability?

4. What should be the contractual obligations of ICANN accredited registrars with regard to accredited privacy/proxy service providers? Should registrars be permitted to knowingly accept registrations where the registrant is using unaccredited service providers that are bound to the same standards as accredited service providers?

In reviewing the Category A questions, the WG agreed that the following sub-question could also be relevant to its deliberations:

- What are obligations of a registrar when it finds out that a registrant is operating as an unaccredited service provider after registration has already been processed?

The WG also agreed that discussion of Question A-3 should take place later on in its deliberative processes, given that the 2013 RAA only went into effect on 1 January 2014. It is expected that the WG will return to this question following the close of the public comment period on this Initial Report. The

WG also did not develop preliminary recommendations for Questions A-1 or A-4, as these appear to be general questions that would be better addressed following the WG's finalization of all its specific recommendations in the other Charter question categories.

The WG's preliminary conclusions on Category A can be found in Section 7.

5.3 Maintenance of Privacy/Proxy Services (Charter Questions Grouping Category B)

The following Charter questions were grouped into this Category B, with an additional sub-questions agreed on and added to Question B-2 as indicated below:

1. Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made through a privacy/proxy service?
2. Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?
   a) *How would such checks be conducted and to what level (e.g., following the levels of validation and verification set out in the 2013 Registrar Accreditation Agreement or some other level)?*
3. What rights and responsibilities should domain name registrants that use privacy/proxy services have? What obligations should ICANN-accredited privacy/proxy service providers have in managing these rights and responsibilities? Clarify how transfers, renewals, and PEDNR policies should apply.

In relation to Question B-3, the WG requested a briefing from ICANN staff on the current policies and processes regarding transfers, renewals and post-expiration domain name recovery (PEDNR). The WG also created a Sub-Team to consider issues that might arise during domain name transfers, including transfers from a failed registrar and inter-registrar transfers where either the gaining or losing registrar uses a privacy or proxy service. The Sub-Team recommended[32] that the WG consider generally mandating the relay of ICANN-critical communications (such as required notices and reminders – for

[32] See the Sub-Team report on transfer issues: https://community.icann.org/x/BI-hAg.

example, annual reminders under the WHOIS Data Reminder Policy and notices under the Expired Registrations Recovery Policy). For transfers from a failed or de-accredited registrar, the Sub-Team considered that the situation would be almost fully covered by ICANN's Inter-Registrar Transfer Policy ("IRTP").

In analysing the interplay between privacy protections (via use of a privacy/proxy service) and the process of a transfer under the IRTP, the Sub-Team noted several types of use cases that could take place, as follows:

A. Non-Private to Non-Private (Current IRTP)	B. Private to Non-Private
C. Non-Private to Private	D. Private to Private

0 No P/P service involvement, (status quo under current IRTP)
1 Losing registrar has affiliated P/P, Gaining does not.
2 Gaining registrar has affiliated P/P, Losing does not.
3 Both Gaining and Losing registrars have affiliated P/P which the customer has opted to use.

The Sub-Team noted that cases arising under B and D would likely require some method for registrars and their affiliated privacy/proxy services to exchange protected contact data, such as a hash function, in order to provide additional protection for the transfer of the domain name.

The WG's preliminary conclusions on Category B can be found in Section 7.

5.4 Registration of Privacy/Proxy Services (Charter Questions Category C)

The following Charter questions were grouped into this Category C, with the WG agreeing early on that an additional "threshold" question was needed to more fully contextualize the question of "commercial" and "non-commercial" use. As with other Charter categories, the WG also agreed on a number of sub-questions for discussion within this category.

Threshold Question:

Currently, proxy/privacy services are available to companies, non-commercial organizations and individuals. Should there be any change to this aspect of the current system in the new accreditation standards?[33]

1. Should ICANN-accredited privacy/proxy service providers distinguish between domain names used for commercial vs. personal purposes? Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes?
   a) *Define "commercial purpose" – must there be actual "trading", or does it include any online business purpose (e.g. including for information or education)?*
   b) *Should there be a definition of what constitutes trading? Purpose? Level?*
   c) *Any difference between "personal" vs "noncommercial" e.g. what about noncommercial organizations or noncommercial purposes such as political, hobby, religious or parental?*
   d) *Include whether registration is for commercial purpose (not just the use of the domain name)*
   e) *Must P/P services disclose affiliated interests?*
2. Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?
   a) *What about non-profits and other noncommercial organizations that use a domain name for noncommercial purposes?*
3. Should there be a difference in the data fields to be displayed if the domain name is registered or used[34] for a commercial purpose, or by a commercial entity instead of a natural person?
   a) *Registration AND (not OR) use?*

   b) How to deal with non-commercial organizations that may be incorporated as corporations for insurance or liability purposes?

This Charter category generated a significant amount of discussion within the WG, primarily due to the lack of a clear definition or distinction as to what might constitute "commercial" and "non-commercial"

[33] Several WG members noted that some questions in this Category C are somewhat conditional, in that a Yes/No answer to one may obviate the need to answer others.

[34] It was suggested during the WG deliberations over Category C that a further threshold question could be whether enquiring into "use" of a domain name is within ICANN's scope and mission.

purposes, uses and organizations. Concern was also expressed over whether enquiring into the "use" of a domain name might implicate content issues. As of this writing, the WG's preliminary conclusions on Category C are divided into a majority and a minority view, for which the WG solicits public comment to assist it in preparing for a consensus call as it developms a Final Report following its review of any public comments received.

The current majority/minority positions of the WG on the questions in this Category C can be found in Section 7.

5.5 Provision of Contact Point by a Privacy/Proxy Service (Charter Questions Category D)

The following Charter questions were grouped into this Category D, with the WG agreeing on additional sub-questions as shown below.

1. What measures should be taken to ensure contactability and responsiveness of the providers?
2. Should ICANN-accredited privacy/proxy service providers be required to maintain dedicated points of contact for reporting abuse? If so, should the terms be consistent with the requirements applicable to registrars under Section 3.18 of the RAA?
3. Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?
4. What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider[35]?

   a) Difference between "illegal" and "malicious"?

   b) Any difference if requestor is law enforcement vs. private party; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant's respective jurisdictions?

In its deliberations on Category D, the WG noted that the current interim Privacy/Proxy Specification in the 2013 RAA requires providers to "publish a point of contact for third parties wishing to report abuse

[35] Several WG members pointed out that having a published point of contact may mean that it will be used for both legitimate as well as spurious purposes.

or infringement of trademarks (or other rights)". The WG also reviewed the current requirements applicable to accredited registrars under Section 3.18 of the 2013 RAA, noting the difference between a contact point that is "designated" as opposed to one that is "dedicated" to receive reports and complaints. The WG also discussed the relevance of the definition of "illegal activity" in the 2013 RAA, and agreed that it may be helpful to analyse the possible difference (and consequent impact) between the phrase "illegal activity" and "malicious conduct".

The WG's preliminary conclusions on Category D can be found in Section 7.

5.6 Relay of Communications to a Privacy/Proxy Service Customer (Charter Questions Category E)

The following Charter questions were grouped into this Category E, with several additional sub-questions agreed on by the WG.

1. What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers?
2. Should ICANN-accredited privacy/proxy service providers be required to forward to the customer all allegations of illegal activities they receive relating to specific domain names of the customer?
    a) *If so, should this apply to all formats, or just email communications?*
    b) *Plus publication of email address of the complainant?*
    c) *Any difference if enquiry is from law enforcement, private attorney or other parties?*
    d) *Should the P&P Service refrain from forwarding the allegations to the customer if the enquire asks not to do it and reasons its request?*
    e) *Any difference; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant's respective jurisdictions?*
    f) *If allegations are received from supposed victim, how to protect her safety/privacy? Require redacted (i.e. identifying information is removed) requests or have this as an option?*
    g) *Should P/P service have discretion to forward rather than be mandated (outside a court order or law enforcement request)?*

Concerns surrounding the lack of rules and standard practices for the relaying of third party communications to a privacy or proxy service customer – as well as the revealing of customer identities and contact information – have been well documented previously, including most recently by the WHOIS RT and the EWG (see Section 3, above). A specific example relevant to relay and reveal procedures would be the GNSO's 2010 deliberations over a proposal to study the extent to which legitimate uses of WHOIS data were curtailed by privacy and proxy services. These discussions revealed significant concerns over the feasibility of such a study, largely because of a likely inability to obtain a sufficient data sample from volunteer respondents for reasons ranging from business sensitivities to privacy implications[36].

The GNSO Council therefore commissioned a feasibility survey, to be conducted by the Interisle Consulting Group. The survey findings, published in August 2012, suggested that "a full study would have to be designed and carried out in a way that did not require participants to disclose specific details of domain names or identify registrants using privacy/proxy services. A full study that depended on the ability to track and correlate individually identifiable requests and responses would therefore be impractical. A study designed to work with anonymized or aggregated request data would be acceptable to at least some potential participants if strong assurances were provided that their data would be protected and their participation would not require substantial time and effort. Anonymized or aggregated data, however, might not support the type of detailed analysis expected by the GNSO Council. Careful consideration of this tradeoff should precede any decision to invest in a full study."

The GNSO Council did not proceed with a full study on relay procedures and the use of privacy or proxy services. As a result, the PPSAI WG's discussions of its chartered tasks with respect to relay procedures as well as reveal issues (see, further, Section 5.7 below) consumed a significant amount of the WG's time. The issues surrounding relay and reveal also formed a substantial part of the agenda for the WG's facilitated face-to-face full-day meeting that took place in in Los Angeles in October 2014, immediately before ICANN's 51st Public Meeting.

[36] See http://gnso.icann.org/en/issues/whois/whois-pp-relay-reveal-feasibility-survey-28mar11-en.pdf.

Nevertheless, the WG was able to come to agreement preliminarily regarding the relaying (or forwarding) by a provider of electronic communications. In dealing with the possibility that a third party requestor might not receive a response, the WG distinguished between a situation where a customer does not respond to a request received (i.e. no response) and one where a customer does not receive the request (i.e. non-delivery). In this regard, the WG noted that different systems may be configured differently, and a provider may not know in many cases that delivery to a customer has failed or been delayed. The WG therefore agreed to craft its recommendations in technologically neutral language, to allow for multiple types of situations of delivery failure, and to condition provider action upon knowledge of persistent delivery failure. The WG also noted that the current interim Privacy/Proxy Specification in the 2013 RAA obligates ICANN-accredited registrars and their Affiliates and Resellers who offer privacy or proxy services to disclose in their terms of service the circumstances under which it will relay third party communications to a customer.

In addition, the WG discussed the question of escalation, and the extent of a provider's obligation to act in the event that a requestor does not receive a response to its request from a customer. It was noted that escalation requests could be in either electronic or hard copy form, and there may be a cost associated with dealing with various different formats. The WG also acknowledged its recommendation under Category B – to the effect that a provider has an obligation to verify the accuracy of a customer's contact information upon becoming aware that attempted delivery of a communication has failed[37]. The WG therefore attempted to craft preliminary recommendations that would balance the various different interests involved in dealing with a relay request and consequent escalation procedures.

The WG's preliminary conclusions on this Category E can be found in Section 7.

5.7 Reveal of a Privacy/Proxy Customer's Identity or Contact Details in WHOIS (Charter Questions Category F)

The following Charter questions were grouped into this Category F, with some additional sub-questions agreed on by the WG.

[37] See the WG's preliminary conclusion on this point, under Charter Category Questions B-2 and B-3 (Section 6, below).

1. What, if any, are the baseline minimum standardized reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
   a) Any difference if requestor is law enforcement or a private party?
   b) Should details of the complainant be revealed to the registrant/owner?
   c) Consider a voluntary cancellation of the domain name registration as an option, notwithstanding access to data by legitimate requestors. If so, should law enforcement and injured parties still have access to the information? How (if at all) to prevent registrant from changing her information upon receiving notification?
   d) *Consider customer option for different methods and notification issues where applicable laws so permit.*
   e) What processes or levels of revealing the underlying registrant exist?
   f) What are the minimum standards of proof that should be required for the identity of the requestor?
   g) What are the minimum standards of proof that should be required for the allegations being raised by the requestor?
   h) Does the P&P service have to assess the lawfulness of the request? What if the allegation refers to conduct legal in one jurisdiction but not the other?
   i) What limitations should the requestor be required to agree to regarding use of the revealed data (e.g., only for the purpose stated in the request and not for publication to the general public)?
2. Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for the specific purpose of ensuring timely service of cease and desist letters?
   a) When should P/P providers be required to do this?
   b) Clarify that this relates to service of letters by private attorneys (and other parties?)
   c) *Should notification of the customer also/ be required?*
   d) When should customer be notified? Under what circumstances can customer contest the reveal before it takes place?
   e) Any difference if requestor is law enforcement vs. private party; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant's respective jurisdictions?
3. What forms of alleged malicious conduct, if any, and what evidentiary standard would be

sufficient to trigger a reveal?

a) *Any difference if requestor is law enforcement vs. private party; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant's respective jurisdictions?*

4. What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?
   a) *Protections to cover both individuals and organizations*
   b) *Safeguards needed also for small businesses/entrepreneurs against anti-competitive activity, as well as for cases of physical/psychological danger (e.g. stalking/harassment) perhaps unrelated to the purpose of the domain name?*
   c) *Consider protections also for cases where publication of physical address could endanger someone's safety, or the safety of an organization (e.g. a religious or political group)*
5. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
6. What clear, workable, enforceable and standardized processes should be adopted by ICANN-accredited privacy/proxy services in order to regulate such access (if such access is warranted)?
7. What specific alleged violations of the provider's terms of service, if any, would be sufficient to trigger publication of the registrant/owner's contact information?
8. What safeguards or remedies should be available in cases where publication is found to have been unwarranted?
   a) *Should registrant be notified prior to publication?*
9. What are the contractual obligations, if any, that if unfulfilled would justify termination of customer access by ICANN-accredited privacy/proxy service providers?

As noted under Section 5.6 above, previous community work had revealed substantial concerns and a lack of rules and standard practices for whether and when a privacy or proxy service provider reveals – either to a specific third party requestor or more broadly to the public by publishing in WHOIS – a customer's identity or contact details. The WG therefore also spent a significant amount of time discussing this topic, including many of the specific issues highlighted in the various Charter questions in this category.

The WG was able to come to agreement on definitions that more clearly explain the two possible forms of a "reveal", i.e. disclosure to a single requestor as opposed to publication to the world at large. It reviewed a sampling of responses from various privacy and proxy service providers, which confirmed the lack of standard practice among providers in relation to how they handle disclosure and publication requests. The sampling also showed that in the current environment, many providers include provisions in their terms of service that inform customers either of circumstances under which a provider will disclose or publish their identity and/or contact information, or that note a provider's discretion to do so in appropriate situations (e.g. in response to a court order). As with relay, this comports with the current requirement in the interim Privacy/Proxy Specification of the 2013 RAA, in that ICANN-accredited registrars, their Affiliates and Resellers who offer privacy or proxy services are obligated presently to disclose to their customers the circumstances under which a customer's identity or contact details will be disclosed or published. The sampling of privacy and proxy providers did, however, indicate that publication of a customer's details in WHOIS generally were more likely to be a consequence of a provider's terminating[38] its service to a customer as a result of that customer's breach of the terms of service.

One of the specific issues upon which the WG seeks public comment on in this regard is therefore the community's view as to whether the current provisions in the 2013 RAA interim Privacy/Proxy Specification are sufficient, or if additional and/or more specific provisions need to be developed,

The WG also acknowledged that there are various different grounds upon which third parties may request disclosure. These can include the initiation of proceedings under the UDRP, allegations of copyright, trademark or other intellectual property infringement, problems with the content of a website(s), and the distribution of malware. In addition, there are also different types of requestors – such as LEA, intellectual property rights owners or their attorneys, and anti-spam and anti-phishing groups (among others). The WG noted that different standards and recommendations may have to be developed for either each type of request, or each type of requestor, or both.

[38] See further Section 5.8 below.

The WG also acknowledged that a request for disclosure or publication need not be conditioned on there first having been a relay request from that particular requestor. The WG also discussed the likelihood that clear, consistent and well-understood procedures for relay may reduce the need and dependency by requestors on disclosure or publication in order to resolve issues with a domain name.

As of this writing, the WG has yet to develop a full set of preliminary conclusions for Category F. As such, public comments are invited on the current set of potential recommendations as well as the outstanding questions – all listed in Section 7 below. The WG will review all public comments received in developing a final set of proposed recommendations for this and all the other Charter question categories.

5.8 Termination [and De-Accreditation] of Privacy/Proxy Services

The following Charter questions were grouped into this Category G, with additional sub-questions agreed on by the WG:

1. What types of services should be covered, and what would be the forms of non-compliance that would trigger cancellation or suspension?

a) How will disputes about accreditation of a P/P service provider be resolved?

b) What will be the process for complaints that a particular accredited provider no longer satisfies accreditation standards?

c) Would there be an appeal mechanism if a provider is denied accreditation?

The WG agreed early on that the scope of its Charter included deliberation both of the situation where a privacy or proxy service provider terminates service to a customer, as well as that where the privacy or proxy service provider's accreditation is itself terminated by ICANN, i.e. de-accreditation.

The WG also sought and obtained briefings from ICANN's Registrar Services department, in order to understand, first, the process of registrar accreditation and de-accreditation under the 2013 RAA, and secondly, whether or not the registrar accreditation and de-accreditation process might serve as the model for a privacy/proxy services accreditation and de-accreditation program. The WG acknowledged that many of the actual details and procedures regarding such a process will be developed as part of implementation of the WG's policy recommendations; however, the WG also felt that understanding the

various alternative models for accreditation and de-accreditation could help inform its deliberations and development of workable, implementable policy.

The WG's preliminary conclusions for this Category G can be found in Section 7.

6. Community Input

6.1 Request for Input

According to the GNSO's PDP Manual[39], a PDP WG should formally solicit statements from each GNSO Stakeholder Group and Constituency at an early stage of its deliberations. A PDP WG is also encouraged to seek the opinion of other ICANN Supporting Organizations and Advisory Committees who may have expertise, experience or an interest in the issue. As a result, the WG reached out to all ICANN Supporting Organizations and Advisory Committees as well as GNSO Stakeholder Groups and Constituencies with a request for input (see Annexes B and C) at the start of its deliberations. In response, statements were received from:

- The GNSO Business Constituency (BC)
- The GNSO Intellectual Property Constituency (IPC)
- The GNSO Internet Service Provider & Connectivity Provider Constituency (ISPCP)
- The GNSO Non-Commercial Stakeholder Group (NCSG)
- The At-Large Advisory Committee (ALAC)

The full statements can be found here: https://community.icann.org/x/SRzRAg.

6.2 Review of Input Received

All of the statements received were added to the template for each Charter question (where applicable) and reviewed by the WG as part of its deliberations on that particular topic.

[39] See Annex 2 of the GNSO Operating Procedures: http://gnso.icann.org/council/annex-2-pdp-manual-13nov14-en.pdf.

7. Working Group Preliminary Recommendations and Observations

7.1 Preliminary Recommendations

The WG was tasked to provide the GNSO Council with "policy recommendations regarding the issues identified during the 2013 RAA negotiations, including recommendations made by law enforcement and GNSO working groups, that were not addressed during the 2013 RAA negotiations and otherwise suited for a PDP; specifically, issues relating to the accreditation of Privacy & Proxy Services". The following are the preliminary recommendations from the WG, listed in order of each of the Charter questions, as grouped by category (A-G). Where these have yet to be finalized or do not represent a consensus position within the WG, square brackets around specific options under consideration have been used to indicate the current thinking of the WG; where there is a majority and a minority view on a particular issue, both viewpoints have been included.

CATEGORY A QUESTION 2[40]: Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?

WG Preliminary Conclusion: ***Privacy and proxy services could potentially be treated the same way for the purpose of the accreditation process.***

CATEGORY B QUESTION 1 - Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made through a privacy/proxy service?

WG Preliminary Conclusion: ***Domain name registrations involving privacy/proxy service providers should be clearly labeled as such in WHOIS[41].***

[40] The WG has deferred consideration of Questions A-1, A-3 and A-4 pending the results of public comment and further analysis on the specific Charter questions in Categories B through G.
[41] The WG acknowledged that implementing this recommendation may require analysis of possible implications of adding another field to WHOIS.

WG Notes on B-1:

There may be various ways to implement this recommendation in order to achieve this objective; the feasibility and effectiveness of these options should be further explored as part of the implementation process. As an example, it was suggested that P/P services could be required to provide the registration data in a uniform / standard format that would make it clear that the domain name registration involves a P/P service - e.g. entering in the field for registrant information 'Service Name, on behalf of customer' (in the case of a proxy service this could then include a number, customer #512, while in the case of a privacy service it would include the actual customer name). Following submission of this information to the registrar, this information would then be displayed in WHOIS making it clearly identifiable as a domain name registration involving a P/P service.

CATEGORY B QUESTION 2 - Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?

WG Preliminary Conclusion: ***The WG recommends[42] that proxy and privacy customer data be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Specification of the 2013 RAA. Moreover, in the cases where validation and verification of the P/P customer data was carried out by the registrar, re-verification by the P/P service of the same, identical, information should not be required.***

WG Notes on B-2:

Similar to ICANN's WHOIS Data Reminder Policy, P/P providers should be required to inform the P/P customer annually of his/her requirement to provide accurate and up to date contact information to the P/P provider. If the P/P service has any information suggesting that the P/P customer information is incorrect (such as P/P service receiving a bounced email notification or non-delivery notification message in connection with compliance with data reminder notices or otherwise) for any P/P customer, the P/P provider must verify or re-verify, as applicable, the email address(es). If, within fifteen (15)

[42] Some WG members are of the view that the minimum verification or validation standards for accredited services would need to exceed those applicable to non-proxy registrations, but this view could be affected by the outcome of discussions regarding relay and reveal requirements (e.g., re the speed of reveal). As such, this recommendation will be revisited upon the completion of the WG deliberations on the other Charter questions.

calendar days after receiving any such information, P/P service does not receive an affirmative response from the P/P customer providing the required verification, the P/P service shall verify the applicable contact information manually.

CATEGORY B QUESTION 3 - What rights and responsibilities should domain name registrants that use privacy/proxy services have? What obligations should ICANN-accredited privacy/proxy service providers have in managing these rights and responsibilities? Clarify how transfers, renewals, and PEDNR policies should apply?

WG Preliminary Conclusion: ***All rights, responsibilities and obligations for registrants as well as privacy/proxy providers would need to be clearly communicated in the privacy/proxy registration agreement, including any specific requirements applying to transfers and renewals. Further details as to minimum requirements for rights, responsibilities and obligations may need to be developed.***

The WG also recommends that the following mandatory requirements form part of a P/P service accreditation program:

- ***All P/P services must relay to their customers any notices required under the RAA or an ICANN Consensus Policy.***
- ***All P/P service registration agreements must state the customer's rights and responsibilities and the P/P service's obligations in managing those rights and responsibilities. Specifically, all P/P services must disclose to their customers the conditions under which the service may be terminated in the event of a transfer of the domain name.***

In addition, the WG recommends the following as best practices:

- ***P/P services should facilitate and not hinder the transfer, renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the ERRP and transfers to another P/P service.***
- ***P/P services should use commercially reasonable efforts to avoid the need to disclose underlying customer data in the process of renewing, transferring or restoring a domain name.***

WG Notes on B-3:

In relation to transfers and renewals, the WG noted the common practice of terminating privacy/proxy protection as part of the transfer process and recommends that this be clearly disclosed to registrants (NOTE: a sub group was formed to explore practical ways to facilitate transfers without the need for termination – see Section 5.3, above).

The WG may further explore the possibility of recommending that P/P providers report updates to WHOIS information within a certain time frame (e.g. modelled on Section 3.2.2 of the 2013 RAA).

CATEGORY C[43]:

"Threshold" Question: Currently, proxy/privacy services are available to companies, non-commercial organizations and individuals. Should there be any change to this aspect of the current system in the new accreditation standards[44]?

The WG discussed the practical difficulties created by the lack of clear definition as to what is "commercial" and what is "non-commercial". For instance, a distinction could be made on the basis of the individual or organization having a certain corporate form, or on the basis of the activities/transactions the individual or organization engages in regardless of corporate form. In addition, some commercial entities register and use domain names for non-commercial (e.g. charitable or experimental) purposes.

The WG agrees that the status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether proxy/privacy services are

[43] The WG agreed to first discuss a Threshold (i.e. baseline) Question for this Category. In the course of deliberations it became clear that likely responses to Questions C-1 & C-2 were closely linked to this Threshold Question.

[44] In agreeing to first discuss this threshold question for Category C, WG members noted also that answers to some questions in this category might be somewhat conditional, in that a Yes/No answer to one may obviate the need to answer others. The WG also noted that references to the "use" of a domain for specific purposes may also implicate content questions.

available to the registrant. Fundamentally, P/P services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals[45].

However, a minority of WG members is of the view that domain names being actively used for commercial transactions (e.g., the sale or exchange of goods or services) should not be able to use or continue using proxy/privacy services. Accordingly, Charter Question C-1 presents some distinctions that create a division within the WG, and for which public comments are sought by the WG.

CATEGORY C QUESTION 1 - Should ICANN-accredited privacy/proxy service providers distinguish between domain names used for commercial vs. personal purposes? Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes?

As noted above, the WG agrees that the mere fact of a domain being registered by a commercial entity, or by anyone conducting commercial activity in other spheres, should not prevent the use of P/P services. In addition, a majority of WG members did not think it either necessary or practical to prohibit domain names being actively used for commercial activity from using P/P services.

However, a minority of WG members disagreed, noting that in the "offline world" businesses often are required to register with relevant authorities as well as disclose details about their identities and locations. These members expressed the view that it is both necessary and practical to distinguish between domains used for a commercial purpose (irrespective of whether the registrant is actually registered as a commercial entity anywhere) and those domains (which may be operated by commercial entity) that are used for a non-commercial purpose. However, domains that conduct financial transactions online must have openly available domain registration information for purposes of, for example, consumer self-protection and law enforcement purposes. Accordingly, these members suggested that domains used for online financial transactions with a commercial purpose should be ineligible for privacy and proxy registrations.

Among the arguments in response, some WG members assert that in jurisdictions where similar legal

[45] [45] The WG notes that the WHOIS RT had specifically acknowledged that privacy and proxy services can be and are used to address legitimate interests, both commercial and non-commercial.

requirements (e.g. business registration, disclosure of location) already exist for the "online world", such disclosures are generally made via a prominent link on the web site rather than in the WHOIS data. This is due apparently to the fact that, in the translation from the "offline world" to the "online world", legislators usually focus on the content available under the domain name, not the domain name registration itself. The majority view also holds that there may be valid reasons why domain name registrants using their domain names for commercial purposes may legitimately need the availability of such services (for example, for the exercise of political speech).

Question C-1 subparts (a) and (b), which the WG added to focus its discussions, suggest defining "commercial" within the context of specific activities, and uses "trading" as an example. However, the WG discussion has focused on a broad term "commercial" and whether certain types of commercial activity mean that a domain is not eligible for P/P registration. The WG therefore began to use the word "commercial" in a broad sense and the word "transactional" to address issues raised by the position held by the minority group on the threshold question.

Accordingly, the WG chairs developed a possible definition of "transactional" for further discussion of the minority group's approach, as follows: ***"[D]omains used for online financial transactions for commercial purpose should be ineligible for privacy and proxy registrations."***.

CATEGORY C QUESTION 2 - Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?

Given the foregoing discussion, ***the WG does not believe that privacy/proxy registrations should be limited to private individuals who use their domains for non-commercial purposes.***

WG Notes on C-1 & C-2:

The WG notes that per its preliminary agreement on question B-1, "domain name registrations involving privacy/proxy service providers should be clearly labeled as such in WHOIS. The WG observes that there may be various ways to implement this recommendation in order to achieve this objective and suggests that the feasibility and effectiveness of these options is further explored as part of the implementation process … "

CATEGORY C QUESTION 3 - Should there be a difference in the data fields to be displayed if the domain name is registered or used for a commercial purpose, or by a commercial entity instead of a natural person?

WG Preliminary Conclusion: ***A majority of WG members are of the view that it is neither desirable nor feasible to make a distinction in the data fields to be displayed.***

Additional Questions for the Community on Category C:
Should the majority or minority view of the WG be adopted? Should a definition of "commercial" or "transactional" be adopted (per the WG Chairs' suggested definition or some other)? Should there be a distinction in the data fields to be displayed as a result?

CATEGORY D QUESTION 1- What measures should be taken to ensure contactability and responsiveness of the providers?

WG Preliminary Conclusion: ***ICANN should publish and maintain a publicly accessible list of all accredited P/P providers, with all appropriate contact information. Registrars should provide a web link to P/P services run by them or their Affiliates, and P/P providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program.***

WG Notes and Additional Questions for the Community on D-1:
The WG noted that responsiveness is a separate and necessary part of the accreditation program, but has not finalized agreement on the appropriate form and level of responsiveness to be required of accredited P/P providers (see D-2 discussion, below).

CATEGORY D – QUESTION 2: Should ICANN-accredited privacy/proxy service providers be required to maintain dedicated points of contact for reporting abuse? If so, should the terms be consistent with the requirements applicable to registrars under Section 3.18 of the RAA?

WG Preliminary Conclusion: ***The WG agreed that a "designated" rather than a "dedicated" point of contact will be sufficient for abuse reporting purposes, noting that the primary concern is to have one contact point that third parties can go to and expect a response from.***

WG Notes and Additional Questions for the Community on D-2:

The WG noted that the TEAC language of "capable and authorized" could be helpful as a possible standard for a designated contact. On responsiveness, the WG agreed to further discuss the sufficiency of a "reasonable and prompt" standard (per Section 3.18 of the 2013 RAA) under the Relay and Reveal categories.

The WG also noted with approval the following recommendations from ICANN's Compliance Department (whose input the WG had sought in relation to the practical workings of Section 3.18 to date), and agreed they may be helpful in its further review of this question: (i) provide guidance to an abuse report requirement as to the types of abuse complaints allowed and types of actions P/P providers should take about these reports; and (ii) consider alternative abuse report options other than publishing an email address on a website and in WHOIS output (to address increasing volumes of spam).

Questions:

What should be the standard for maintaining a designated point of contact – "reasonable and prompt" (per the TEAC) or other? What should be required of P/P providers in terms of level of responsiveness – "reasonable and prompt" (per the 2013 RAA) or other?

CATEGORY D QUESTION 3 - Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?

WG Preliminary Conclusion: ***The WG agreed that P/P providers should be fully contactable; it has yet to reach agreement on whether adopting Section 2.3 (from the 2013 RAA Temp Spec) will be sufficient in this regard.***

WG Notes and Additional Questions for the Community on D-3:

The WG notes that it is likely to make other recommendations in response to other Charter questions that may affect this issue (e.g. the WG recommendation for ICANN to publish a publicly-accessible list of accredited providers (see WG Preliminary Conclusion for D-1), and for WHOIS entries to be clearly labeled if they are those of a P/P provider (see WG Preliminary Conclusion for B-1).)

Question:

Should the standard for provider contactability be the same as that under Section 2.3 of the 2013 RAA?

CATEGORY D QUESTION 4 - What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?

WG Preliminary Conclusion: ***The WG recommends that the requirements in relation to which forms of alleged malicious conduct would be covered by the designated published point of contact at an ICANN-accredited privacy/proxy service provider include a list of forms of malicious conduct to be covered. These requirements should allow for enough flexibility to accommodate new types of malicious conduct. Section 3 of the Public Interest Commitments (PIC) Specification in the New gTLD Registry Agreement[46] or Safeguard 2, Annex 1 of the GAC's Beijing Communique[47] could serve as examples for how this could be achieved.***

The WG also recommends that a standardized form for information requests and reports be developed, to also include space for free form text[48]. It was also suggested that providers should have the ability to "categorize" reports received, in order to facilitate responsiveness.

---

[46] "Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."

[47] "Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law."

[48] The WG discussed but did not finalize the minimum elements that should be included in such a form.

CATEGORY E QUESTIONS 1 & 2 - What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers? Should ICANN-accredited privacy/proxy service providers be required to forward to the customer all allegations of illegal activities they receive relating to specific domain names of the customer?

WG Preliminary Conclusions: The WG divided its discussions on Category E into two further topics, as further detailed below:

I. Regarding Electronic Communications[49]:

(1) All communications required by the RAA and ICANN Consensus Policies must be forwarded;

(2) For all other electronic communications, providers may elect one of the following options:

- ***Option #1: Forward all electronic requests received (including emails and via web forms), but the provider may implement commercially reasonable safeguards (including CAPTCHA) to filter out spam and other forms of abusive communications***
- ***Option #2: Forward all electronic requests (including those received via emails and web forms) received from law enforcement authorities and third parties containing allegations of domain name abuse (i.e. illegal activity); and***

(3) In all cases, providers must publish and maintain a mechanism (e.g. designated email point of contact) for requestors to contact to follow up on or escalate their original requests.

The WG also recommends that standard forms and other mechanisms that would facilitate the prompt and accurate identification of a relay request be developed for the use of accredited providers (e.g. drop-down menus in a provider's web-based forms or fields that would require the filling in of a requestor's contact details, specifying the type of request or other basic information).

II. Regarding Further Provider Actions When There Is A Repeated Failure of Electronic Communications[50]

[49] The WG agrees that emails, web forms and automated telephone calls would be considered "electronic communications" whereas human-operated faxes and non-automated telephone calls would not. The WG recommends that implementation of the concept of "electronic communications" be sufficiently flexible to accommodate future technological developments.

- ***All third party electronic requests alleging abuse by a P/P customer will be promptly forwarded to the customer. A requestor will be promptly notified of a persistent failure of delivery[51] that a provider becomes aware of.***
- ***The WG considers that a "persistent delivery failure" will have occurred when an electronic communications system abandons or otherwise stops attempting to deliver an electronic communication to a customer after [a certain number of] repeated or duplicate delivery attempts within [a reasonable period of time]. The WG emphasizes that such persistent delivery failure, in and of itself, is not sufficient to trigger further provider obligation or action under this Category E unless the provider also becomes aware of the persistent delivery failure.***
- ***As part of an escalation process, and when the above-mentioned requirements concerning a persistent delivery failure of an electronic communication have been met, the provider [should] [must] upon request forward a further form of notice to its customer. A provider should have the discretion to select the most appropriate means of forwarding such a request [and to charge a reasonable fee on a cost-recovery basis]. [Any such reasonable fee is to be borne by the customer and not the requestor]. A provider shall have the right to impose reasonable limits on the number of such requests made by the same requestor.***
- ***A persistent delivery failure to a customer as described herein will trigger the provider's obligation to perform a verification/re-verification (as applicable) of the customer's email address(es), in accordance with the recommendation of this WG under Category B, Question 2.***
- ***These recommendations shall not preclude a provider from taking any additional action in the event of a persistent delivery failure of electronic communications to a customer, in accordance with its published terms of service.***

CATEGORY F:

1. What, if any, are the baseline minimum standardized reveal processes that should be adopted

---

[50] As the following language is still under discussion by the WG, suggested edits/changes to the initial draft language have been indicated with square brackets around them.

[51] The WG notes that failure of "delivery" of a communication is not to be equated with the failure of a customer to "respond" to a request, notification or other type of communication.

by ICANN-accredited privacy/proxy service providers?

2. **Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for the specific purpose of ensuring timely service of cease and desist letters?**
3. **What forms of alleged malicious conduct, if any, and what evidentiary standard would be sufficient to trigger a reveal?**
4. **What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?**
5. **What circumstances, if any, would warrant access to registrant data by law enforcement agencies?**
6. **What clear, workable, enforceable and standardized processes should be adopted by ICANN-accredited privacy/proxy services in order to regulate such access (if such access is warranted)?**
7. **What specific alleged violations of the provider's terms of service, if any, would be sufficient to trigger publication of the registrant/owner's contact information?**
8. **What safeguards or remedies should be available in cases where publication is found to have been unwarranted?**
9. **What are the contractual obligations, if any, that if unfulfilled would justify termination of customer access by ICANN-accredited privacy/proxy service providers?**

The WG has not yet reached final conclusions on some of the Category F Charter questions. Its deliberations and, where applicable, its preliminary conclusions, are set forth below in detail so as to enable commenters to provide tailored and constructive feedback to the WG on issues relating to the "reveal" of a P/P customer's identity and/or contact details.

I. WG Recommended Definitions

The WG's review of a sample of P/P service provider policies as well as of prior ICANN work on this issue indicates that there is currently no consistent, universally-accepted or well-understood single definition of "Reveal" as the word is used by the ICANN community. The WG has developed the following definitions to cover the two aspects of what a "Reveal" request is commonly understood to

mean, and recommends that ICANN adopt these definitions in its P/P Service Provider Accreditation Program, and in any relevant contracts and related policies:

- ***"Publication" means the reveal of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details in the WHOIS system.***
- ***"Disclosure" means the reveal of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details to a third party requestor without Publication in the WHOIS system.***
- ***The term "person" as used in these definitions is understood to include natural and legal persons, as well as organizations and entities.***

The WG also agreed that there may be a need in certain circumstances to differentiate between a request made by law enforcement authorities (LEA) and one made by other third parties such as intellectual property rights holders or private anti abuse organizations. ***The WG notes that a definition of LEA appears in the 2013 RAA (see https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en) and recommends adopting the same definition in the ICANN Accreditation Program, and in related contracts and policies:***

> ***"Law enforcement authority" means law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the P/P service provider is established or maintains a physical office[52].***

II. General Recommendations on Publication and Disclosure

The WG reviewed the Publication and Disclosure practices of several P/P service providers, some of whom are represented in the WG. Most providers reported using a manual rather than an automated system to deal with Disclosure requests, in the sense that an employee initially reviews a request prior to a decision being made on whether to comply. For at least one provider, its policies and

[52] This is based on the wording of Section 3.18.2 of the 2013 RAA.

practices were intended to encourage the requestor and the customer to deal directly with each other as far as possible.

The WG agreed that none of its recommendations should be read as being intended to alter (or mandate the alteration of) the prevailing practice among providers to review requests manually or to facilitate direct resolution of an issue between a requestor and a customer. It also notes that disclosure of at least some contact details of the customer may in some cases be required in order to facilitate such direct resolution.

The WG has not yet finalized a conclusion on whether to recommend uniform minimum standards for providers to apply in determining when to Disclose or Publish, or in verifying a requestor's identity.

The WG agrees that there can be significant differences between the consequences of Publication of a customer's details in the public WHOIS system compared to Disclosure of the same details to a single third party requestor. Specifically, the WG agrees that there may be a greater need for safeguards to ensure customer protection with respect to Publication than with respect to Disclosure. ***The WG therefore recommends that accredited providers should indicate clearly in their terms of service when referring to Publication requests (and their consequences) and when to Disclosure requests (and their consequences). The WG further recommends that accredited providers expressly include a provision in their terms of service explaining the meaning and consequences of Publication.***

The WG notes that several providers currently include in their terms of service or other published policies provisions pursuant to which the provider may Disclose or Publish a customer's details, or suspend or terminate service to a customer. Possible circumstances include where action is required by legal process such as court orders, subpoenas, or warrants, by ICANN Consensus Policy or by Registry requirements. Occasions also may arise in the course of resolving third party claims involving the domain name or its uses, including where necessary to protect property or rights, the safety of the public or any person, or to prevent or stop activity that may be illegal or unethical. ***Without mandating that such specific provisions be included in an accredited provider's terms of service, the WG nonetheless recommends that accredited providers should indicate clearly in their terms of service the***

specific grounds upon which a customer's details may be Disclosed or Published or service suspended or terminated[53].

The WG further recommends that, in deciding whether or not to comply with a Disclosure or Publication request, providers not mandate that the requestor must have first made a Relay request.

III. WG Recommendations Specific to LEA Requests

[TBA – including whether accredited providers must comply with express LEA requests not to notify a customer, whether there should be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity, and what (if any) remedies there can or should be for unwarranted Publication]

Questions for the Community:

Should it be mandatory for accredited P/P providers to comply with express LEA requests not to notify a customer? Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity? What (if any) should the remedies be for unwarranted Publication?

IV. WG Recommendations Specific to Other Third Party Requests

[TBA – including whether accredited providers must comply with express requests for Disclosure for the purpose of sending cease and desist letters or notices of formal legal proceedings against the customer, and whether customer notification in such cases is to be mandatory]

Questions for the Community:

[53] The current interim P/P Specification in the 2013 RAA requires that P/P providers who are, or who are Affiliated with, Registrars post their terms of service either on their, or on their Affiliated providers' websites, including the circumstances under which they terminate service and when they reveal or disclose the customer's identity and details: see Section 2.4 of the Specification: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#privacy-proxy.

Should it be mandatory for accredited P/P providers to comply with express requests for Disclosure for the purpose of sending cease and desist letters or notices of formal legal proceedings against the customer? Should customer notification in such cases be mandatory?

Further Note:
See Section VII, below, for additional draft language under discussion by the WG relating to requests from intellectual property owners. Note also that the WG may need to further discuss the need for specific and potentially different standards relating to requests from other types of third parties (e.g. anti-abuse groups).

V. WG Recommendations on Customer Notification and the Availability of Alternative Options

The WG recommends that accredited providers should indicate clearly, in their terms of service and on their websites, whether or not a customer: (1) will be notified when a provider receives a Publication or Disclosure request from a third party; and (2) in the case of Publication, whether the customer may opt to cancel its domain registration prior to and in lieu of Publication.

VI. WG Recommendations on Requestor Notification

The WG recommends that accredited providers should indicate clearly, on their websites and in all Publication or Disclosure-related materials, that a requestor will be notified in a timely manner of the provider's decision: (1) to notify its customer of the request; and (2) whether or not the provider agrees to comply with the request to Disclose or Publish.

VII. WG Recommendations on Categorizing Third Party Requests and the Use of Standard Request Forms

The WG's review of provider policies shows that least one provider has in place distinct policies dealing specifically with different types of claims for which a Disclosure request is made, e.g. UDRP Filings, Trademark & Copyright Infringement Complaints, and Subpoenas (Civil and Criminal). The WG believes that such categorization can be a voluntary best practice to be recommended to providers, but does not presently recommend mandating this as a requirement for the Accreditation Program.

Nonetheless, ***the WG recommends that ICANN's Accreditation Program include a requirement for all accredited providers to include on their websites, and in all Publication or Disclosure-related policies and documents, a link to a [standardized] Request Form or an equivalent list of specific criteria that the provider requires in order to comply with such requests.***

VII. Proposed Draft Language relating to Disclosure to Third Party Requestors who are Intellectual Property Rights Holders or Legal Representatives Thereof

- Provider to notify customer when it receives a Disclosure request relating to an "IP complaint stated with great specificity, including the identity of the IP rights holder and complainant, the right(s) involved, and the nature of the infringing activity"[54].
- There should be a period (of X number of days?) for the customer to take action in response to the notification. This may take the form of a direct response to the requestor, a request to cancel its domain name registration, file with a court or other actions.
- Provider [may] [shall] proceed to Disclose if customer does not take responsive action within the specified time frame (but how would provider know that customer has done so? Perhaps require that customer acknowledge receipt of the notification and its intention to take action?)
- Any such Disclosure should be subject to reasonable limitations on the use of such Disclosed information.

CATEGORY G - What types of services should be covered, and what would be the forms of non-compliance that would trigger cancellation or suspension?

The WG discussed the differences between the termination of a P/P provider's accreditation, and the termination by a P/P provider of its service to a customer (e.g. for breach of the provider's terms of service by a customer). The following preliminary conclusions are concerned with the consequences of de-accreditation of a P/P provider.

[54] The quoted language reproduces verbatim language suggested by a WG member.

- ***P/P customers should be notified prior to de-accreditation of a provider, to enable them to make alternative arrangements.*** One possible time in which to do so might be when Compliance sends breach notices to the provider, as customers would then be put on notice (as is done for registrar de-accreditation).
- ***Other P/P providers should also be notified, to enable interested providers to indicate if they wish to become the gaining P/P provider*** (as is done for registrar de-accreditation)
- ***All notification(s) are to be published on the ICANN website*** (as is done for registrar de-accreditation)
- ***A de-accredited P/P provider should have the opportunity to find a gaining provider to work with*** (as sometimes occurs with registrar de-accreditation)
- ***A "graduated response" approach to de-accreditation should be explored***, i.e. a set series of breach notices (e.g. up to three) with escalating sanctions, with the final recourse being de-accreditation
- ***A customer should be able to choose its new P/P provider***
- ***The next review of the IRTP should include an analysis of the impact on P/P customers, to ensure that adequate safeguards are in place as regards P/P protection when domain names are transferred pursuant to an IRTP process***

WG Notes on Category G:

In relation to termination of P/P service by a provider to its customer, the WG noted its recommendations under Category F that P/P providers are to publish certain minimum terms regarding Disclosure and Publication in their terms of service. The WG has yet to finalize a position on whether these minimum recommendations are sufficient to facilitate protection of P/P customers in the event of Publication of a customer's details in WHOIS, as a result of termination of P/P service (including where this was due to the customer's breach of a provider's terms of service). The relevant Category F recommendations in this regard are:

- The specific grounds upon which a provider will Publish a customer's details, suspend service, or terminate service

- The meaning (per the WG's definition) of Publication and its consequences

- Whether a customer will be notified when the provider receives a request either for Disclosure or Publication

- In the case of Publication, whether a customer will have the option to cancel its domain name registration prior to and in lieu of Publication

The WG also discussed whether the current registrar accreditation and de-accreditation model might be applicable as a framework for P/P service providers. The WG agreed that there are some significant distinctions between the registrar model and P/P services, e.g. cancellation/transfer of a domain name is not the same as cancellation/transfer of a P/P service, and domain name transfers are governed by the IRTP (an ICANN Consensus Policy). However, there are also many similarities.

The WG has preliminarily concluded that the registrar model with its multiple steps, governed by the RAA, may not be entirely appropriate for P/P services; however, it is a useful starting point from which relevant portions may be adapted to apply to P/P service providers.

8. Conclusions & Next Steps

The WG will complete the next phase of its work and develop its recommendations in a Final Report to be sent to the GNSO Council for review following its analysis of public comments received on this Initial Report.

Annex A - PDP WG Charter

Working Group Charter for a Policy Development Process to Address Privacy & Proxy Services Accreditation Issues arising under the 2013 Registrar Accreditation Agreement

WG Name:	RAA Privacy & Proxy Services Accreditation Issues PDP Working Group	
Section I: Working Group Identification		
Chartering Organization(s):	Generic Names Supporting Organization (GNSO) Council	
Charter Approval Date:	TBD	
Name of WG Chair:	TBD	
Name(s) of Appointed Liaison(s):	TBD	
WG Workspace URL:	TBD	
WG Mailing List:	TBD	
GNSO Council Resolution:	**Title:**	Motion to Approve the Charter for the 2013 Registrar Accreditation Agreement (RAA) Privacy & Proxy Services Accreditation Issues Policy Development Process (PDP) Working Group (WG)
	Ref # & Link:	TBD
Important Document Links:	•	

Section II: Mission, Purpose, and Deliverables

Mission & Scope:

Background

At the ICANN Meeting in Dakar in October 2011 the ICANN Board adopted Resolution 2011.10.18.32 regarding amendments to the Registrar Accreditation Agreement (Dakar RAA Resolution). The Dakar RAA Resolution directed negotiations on amending the 2009 Registrar Accreditation Agreement (RAA) to be commenced immediately, and requested the creation of an Issue Report to undertake a GNSO Policy Development Process (PDP) as quickly as possible to address any remaining items not covered by the negotiations and otherwise suited for a PDP. With the Preliminary Issue Report on RAA Amendments having been published in December 2011, the Final GNSO Issue Report on RAA Amendments was published, following from the Dakar RAA Resolution, on 6 March 2012. On 27 June 2013, the ICANN Board approved the new 2013 Registrar Accreditation Agreement (2013 RAA). Accordingly, the GNSO Council is now proceeding with the Board-requested PDP on the remaining issues identified in the RAA negotiations that were not addressed in the 2013 RAA; specifically, issues relating to the accreditation of Privacy & Proxy Services.

Mission and Scope

This RAA PDP Working Group (WG) is tasked to provide the GNSO Council with policy recommendations regarding the issues identified during the 2013 RAA negotiations, including recommendations made by law enforcement and GNSO working groups, that were not addressed during the 2013 RAA negotiations and otherwise suited for a PDP; specifically, issues relating to the accreditation of Privacy & Proxy Services.

As part of its deliberations on the matter, the RAA PDP WG should, at a minimum, consider those issues detailed in the Staff Briefing Paper published on 16 September 2013. These are:

- *What, if any, are the types of Standard Service Practices that should be adopted and published by ICANN-accredited privacy/proxy service providers?*
- *What, if any, are the baseline minimum standardized relay and reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?*
- *Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for this specific*

purpose?

- *Should ICANN-accredited privacy/proxy service providers be required to forward on to the customer all allegations they receive of illegal activities relating to specific domain names of the customer?*
- *What forms of malicious conduct (if any) and what evidentiary standard would be sufficient to trigger such disclosure? What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?*
- *What specific violations, if any, would be sufficient to trigger such publication? What safeguards or remedies should there be for cases where publication is found to have been unwarranted?*
- *Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?*
- *What are the contractual obligations (if any) that, if unfulfilled, would justify termination of customer access by ICANN-accredited privacy/proxy service providers?*
- *What rights and responsibilities should customers of privacy/proxy services have? What obligations should ICANN-accredited privacy/proxy service providers have in managing these rights and responsibilities? Clarify how transfers, renewals, and PEDNR policies should apply.*
- *Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made through a privacy/proxy service?*
- *Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required? What measures should be taken to ensure contactability and responsiveness of the providers?*
- *Should ICANN-accredited privacy/proxy service providers be required to maintain dedicated points of contact for reporting abuse? If so, should the terms be consistent with the requirements applicable to registrars under Section 3.18 of the RAA?*
- *What are the forms of malicious conduct (if any) that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?*
- *What circumstances, if any, would warrant access to registrant data by law enforcement agencies?*
- *What clear, workable, enforceable and standardized processes should be adopted by ICANN-accredited privacy/proxy services in order to regulate such access (if such access is warranted)?*
- *Should ICANN-accredited privacy/proxy service providers distinguish between domain names used for commercial vs. personal purposes? Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes? Should there be a difference in the data fields to be displayed if the domain name is registered/ used for a commercial purpose or by a commercial entity instead of to a natural person?*

- *Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?*
- *What types of services should be covered, and what would be the forms of non-compliance that would trigger cancellation or suspension of registrations?*
- *Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?*

The following additional issues should also be considered by the WG:

- *What are the effects of the privacy & proxy service specification contained in the 2013 RAA? Have these new requirements improved WHOIS quality, registrant contactability and service usability?*
- *What should be the contractual obligations of ICANN accredited registrars with regard to accredited privacy/proxy service providers? Should registrars be permitted to knowingly accept registrations where the registrant is using unaccredited service providers that are however bound to the same standards as accredited service providers?*

The WG's final recommendations do not need to be limited to formal Consensus Policy recommendations; it may, for example, make recommendations more appropriately covered by a code of conduct or best practices, or through other mechanisms (e.g. as indicated in the GNSO PDP Manual.) The WG should also bear in mind that this PDP is expected to inform ICANN's proposed Action Plan to launch an accredited privacy/proxy program and further ICANN's ongoing efforts to implement recommendations made by the WHOIS Review Team. In addition, the WG should take into account recommendations made by the WHOIS Review Team at as early a stage as possible, and the results of the WHOIS Privacy & Proxy Abuse Study commissioned by the GNSO Council and published for public comment on 24 September 2013: http://www.icann.org/en/news/public-comment/whois-pp-abuse-study-24sep13-en.htm

The WG may also wish to consider forming sub-groups to work on particular issues or sub-topics in order to streamline its work and discussions.

Objectives & Goals:

To develop, at a minimum, an Initial Report and a Final Report regarding the WG's recommendations on issues relating to the accreditation of privacy & proxy services arising in relation to the 2013 RAA, to be delivered to the GNSO Council, following the processes described in Annex A of the ICANN Bylaws and the GNSO PDP Manual.

Deliverables & Timeframes:

The WG shall respect the timelines and deliverables as outlined in Annex A of the ICANN Bylaws and the

PDP Manual. As per the GNSO Working Group Guidelines, the WG shall develop a work plan that outlines the necessary steps and expected timing in order to achieve the milestones of the PDP as set out in Annex A of the ICANN Bylaws and the PDP Manual, and shall submit this to the GNSO Council.

Section III: Formation, Staffing, and Organization

Membership Criteria:

The WG will be open to all interested in participating. New members who join after certain parts of work has been completed are expected to review previous documents and meeting transcripts.

Group Formation, Dependencies, & Dissolution:

This WG shall be a standard GNSO PDP Working Group. The GNSO Secretariat should circulate a 'Call For Volunteers' as widely as possible in order to ensure broad representation and participation in the WG, including:

- Publication of announcement on relevant ICANN web sites including but not limited to the GNSO and other Supporting Organizations and Advisory Committee web pages; and
- Distribution of the announcement to GNSO Stakeholder Groups, Constituencies and other ICANN Supporting Organizations and Advisory Committees

Working Group Roles, Functions, & Duties:

The ICANN Staff assigned to the WG will fully support the work of the Working Group as requested by the Chair including meeting support, document drafting, editing and distribution and other substantive contributions when deemed appropriate.
Staff assignments to the Working Group:

- GNSO Secretariat
- ICANN policy staff members (Mary Wong)

The standard WG roles, functions & duties shall be those specified in Section 2.2 of the GNSO Working Group Guidelines.

Statements of Interest (SOI) Guidelines:

Each member of the WG is required to submit an SOI in accordance with Section 5 of the GNSO Operating Procedures.

Section IV: Rules of Engagement

Decision-Making Methodologies:

The Chair will be responsible for designating each position as having one of the following designations:

- **Full consensus** - when no one in the group speaks against the recommendation in its last readings. This is also sometimes referred to as **Unanimous Consensus.**
- **Consensus** - a position where only a small minority disagrees, but most agree. *[Note: For those that are unfamiliar with ICANN usage, you may associate the definition of 'Consensus' with other definitions and terms of art such as rough consensus or near consensus. It should be noted, however, that in the case of a GNSO PDP WG, all reports, especially Final Reports, must restrict themselves to the term 'Consensus' as this may have legal implications.]*
- **Strong support but significant opposition** - a position where, while most of the group supports

a recommendation, there is a significant number of those who do not support it.

- **Divergence** (also referred to as **No Consensus**) - a position where there is no strong support for any particular position, but many different points of view. Sometimes this is due to irreconcilable differences of opinion and sometimes it is due to the fact that no one has a particularly strong or convincing viewpoint, but the members of the group agree that it is worth listing the issue in the report nonetheless.
- **Minority View** - refers to a proposal where a small number of people support the recommendation. This can happen in response to **Consensus**, **Strong support but significant opposition**, or **No Consensus;** or it can happen in cases where there is neither support nor opposition to a suggestion made by a small number of individuals.

In cases of **Consensus**, **Strong support but significant opposition**, and **No Consensus**, an effort should be made to document variances in viewpoint and to present any **Minority View** recommendations that may have been made. Documentation of **Minority View** recommendations normally depends on text offered by the proponent(s). In all cases of **Divergence,** the WG Chair should encourage the submission of minority viewpoint(s).

The recommended method for discovering the consensus level designation on recommendations should work as follows:

i. After the group has discussed an issue long enough for all issues to have been raised, understood and discussed, the Chair, or Co-Chairs, make an evaluation of the designation and publish it for the group to review.
ii. After the group has discussed the Chair's estimation of designation, the Chair, or Co-Chairs, should reevaluate and publish an updated evaluation.
iii. Steps (i) and (ii) should continue until the Chair/Co-Chairs make an evaluation that is accepted by the group.
iv. In rare cases, a Chair may decide that the use of polls is reasonable. Some of the reasons for this might be:
    - A decision needs to be made within a time frame that does not allow for the natural process of iteration and settling on a designation to occur.
    - It becomes obvious after several iterations that it is impossible to arrive at a designation. This will happen most often when trying to discriminate between **Consensus** and **Strong support but Significant Opposition** or between **Strong support but Significant Opposition** and **Divergence.**

Care should be taken in using polls that they do not become votes. A liability with the use of polls is that, in situations where there is **Divergence** or **Strong Opposition**, there are often disagreements about the meanings of the poll questions or of the poll results.

Based upon the WG's needs, the Chair may direct that WG participants do not have to have their name explicitly associated with any Full Consensus or Consensus views/positions. However, in all other cases and in those cases where a group member represents the minority viewpoint, their name must be explicitly linked, especially in those cases where polls where taken.

Consensus calls should always involve the entire WG and, for this reason, should take place on the designated mailing list to ensure that all WG members have the opportunity to fully participate in the

consensus process. It is the role of the Chair to designate which level of consensus has been reached and to announce this designation to the WG. WG member(s) should be able to challenge the designation of the Chair as part of the WG discussion. However, if disagreement persists, WG members may use the process set forth below to challenge the designation.

If several participants (see Note 1 below) in a WG disagree with the designation given to a position by the Chair or any other consensus call, they may follow these steps sequentially:

1. Send email to the Chair, copying the WG explaining why the decision is believed to be in error.
2. If the Chair still disagrees with the complainants, the Chair will forward the appeal to the liaison(s) from the Chartering Organization (CO). The Chair must explain his or her reasoning in the response to the complainants and in the submission to the liaison(s). If the liaison(s) supports the Chair's position, the liaison(s) will provide their response to the complainants. The liaison(s) must explain their reasoning in the response. If the liaison(s) disagrees with the Chair, the liaison(s) will forward the appeal to the CO. Should the complainants disagree with the liaison(s)'s support of the Chair's determination, the complainants may appeal to the Chair of the CO or their designated representative. If the CO agrees with the complainants' position, the CO should recommend remedial action to the Chair.
3. In the event of any appeal, the CO will attach a statement of the appeal to the WG and/or Board report. This statement should include all of the documentation from all steps in the appeals process and should include a statement from the CO (see Note 2 below).

Note 1: Any Working Group member may raise an issue for reconsideration; however, a formal appeal will require that that a single member demonstrates a sufficient amount of support before a formal appeal process can be invoked. In those cases where a single Working Group member is seeking reconsideration, the member will advise the Chair and/or Liaison(s) of their issue and the Chair and/or Liaison(s) will work with the dissenting member to investigate the issue and to determine if there is sufficient support for the reconsideration to initiate a formal appeal process.

Note 2: It should be noted that ICANN also has other conflict resolution mechanisms available that could be considered in case any of the parties are dissatisfied with the outcome of this process.

Status Reporting:

As requested by the GNSO Council, taking into account the recommendation of the Council liaison(s) to the WG.

Problem/Issue Escalation & Resolution Processes:

The WG will adhere to ICANN's Expected Standards of Behavior as documented in Section F of the ICANN Accountability and Transparency Frameworks and Principles, January 2008.

If a WG member feels that these standards are being abused, the affected party should appeal first to the Chair and Liaison(s) and, if unsatisfactorily resolved, to the Chair of the CO or their designated representative. It is important to emphasize that expressed disagreement is not, by itself, grounds for abusive behavior. It should also be taken into account that as a result of cultural differences and language barriers, statements may appear disrespectful or inappropriate to some but are not necessarily intended as

such. However, it is expected that WG members make every effort to respect the principles outlined in ICANN's Expected Standards of Behavior as referenced above.

The Chair, in consultation with the CO liaison(s), is empowered to restrict the participation of someone who seriously disrupts the Working Group. Any such restriction will be reviewed by the CO. Generally, the participant should first be warned privately, and then warned publicly before such a restriction is put into place. In extreme circumstances, this requirement may be bypassed.

Any WG member that believes that his/her contributions are being systematically ignored or discounted or wants to appeal a decision of the WG or CO should first discuss the circumstances with the WG Chair. In the event that the matter cannot be resolved satisfactorily, the WG member should request an opportunity to discuss the situation with the Chair of the CO or their designated representative.

In addition, if any member of the WG is of the opinion that someone is not performing their role according to the criteria outlined in this Charter, the same appeals process may be invoked.

Closure & Working Group Self-Assessment:

The WG will close upon the delivery of the Final Report, unless assigned additional tasks or follow-up by the GNSO Council.

Section V: Charter Document History

Version	Date	Description

Staff Contact:	Mary Wong	Email:	Policy-staff@icann.org

Translations: If translations will be provided please indicate the languages below:											

Annex B – Request for Constituency / Stakeholder Group Statements

Stakeholder Group / Constituency / Input Template

Privacy & Proxy Services Accreditation Issues PDP Working Group

---

PLEASE SUBMIT YOUR RESPONSE AT THE LATEST BY **FRIDAY 28 FEBRUARY 2014** TO THE GNSO SECRETARIAT (gnso.secretariat@gnso.icann.org), which will forward your statement to the Working Group.

The GNSO Council has formed a Working Group of interested stakeholders and Stakeholder Group / Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to consider recommendations in relation to Privacy & Proxy Services Accreditation Issues.

Part of the Working Group's effort will be to incorporate ideas and suggestions gathered from Stakeholder Groups and Constituencies through this template statement that contains questions that the GNSO asked the WG to address. Inserting your responses in this form will make it much easier for the WG to summarize the responses. We have categorized the items in the hope that it adds clarity.

This information will be helpful to the community in understanding the points of view of various stakeholders. Please answer as many questions as you can. In addition, please feel free to add any information you deem important to inform the Working Group's deliberations, even if this does not fit into any of the questions listed below.

A short list of definitions that the Working Group hopes your Stakeholder Group/Constituency will find helpful follows after the list of questions. For further information, please visit the Working Group's Workspace (see https://community.icann.org/x/9iCfAg).

Questions from the Working Group Charter:

I. MAIN ISSUES

1. What, if any, are the types of Standard Service Practices that should be adopted and published by ICANN-accredited privacy/proxy service providers?
2. Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?
3. What are the contractual obligations, if any, that if unfulfilled would justify termination of customer access by ICANN-accredited privacy/proxy service providers?
4. What types of services should be covered, and would be the forms of non-compliance that would trigger cancellation or suspension of registrations?
5. What are the effects of the privacy and proxy service specification contained in the 2013 RAA? Have these new requirements improved WHOIS quality, registrant contactability and service usability?
6. What should be the contractual obligations of ICANN accredited registrars with regard to accredited privacy/proxy service providers? Should registrars be permitted to knowingly accept registrations where the registrant is using unaccredited service providers that are however bound to the same standards as accredited service providers?

II. MAINTENANCE

1. Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made through a privacy/proxy service?
2. Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?
3. What rights and responsibilities should customers of privacy/proxy services have? What obligations should ICANN-accredited privacy/proxy service providers have in managing these rights and responsibilities? Clarify how transfers, renewals, and PEDNR policies should apply.
4. Should ICANN-accredited privacy/proxy service providers distinguish between domain names used for commercial vs. personal purposes? Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes?
5. Should there be a difference in the data fields to be displayed if the domain name is registered or used for a commercial purpose, or by a commercial entity instead of a natural person?
6. Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?

III. CONTACT

1. What measures should be taken to ensure contactability and responsiveness of the providers?
2. Should ICANN-accredited privacy/proxy service providers be required to maintain dedicated points of contact for reporting abuse? If so, should the terms be consistent with the requirements

applicable to registrars under Section 3.18 of the RAA?
3. Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?
4. What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?

IV. RELAY

1. What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers?
2. Should ICANN-accredited privacy/proxy service providers be required to forward to the customer all allegations of illegal activities they receive relating to specific domain names of the customer?

V. REVEAL

1. What, if any, are the baseline minimum standardized reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
2. Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for the specific purpose of ensuring timely service of cease and desist letters?
3. What forms of alleged malicious conduct, if any, and what evidentiary standard would be sufficient to trigger such disclosure? What specific alleged violations, if any, would be sufficient to trigger such publication?
4. What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?
5. What safeguards or remedies should be available in cases where publication is found to have been unwarranted?
6. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
7. What clear, workable, enforceable and standardized processes should be adopted by ICANN-accredited privacy/proxy services in order to regulate such access (if such access is warranted)?

Other information/Suggestions:

****

LIST OF RELEVANT DEFINITIONS

(1) Privacy & Proxy Services

The following definitions are those used by the GNSO in the various WHOIS studies that it commissioned between 2010-2012 (http://gnso.icann.org/issues/whois/whois-working-definitions-study-terms-18feb09.pdf):

- ***Privacy services*** hide customer details from going into WHOIS. Privacy service providers, which may include registrars and resellers, may offer alternate contact information and mail forwarding services while not actually shielding the domain name registrant's identity. By shielding the user in these ways, these services are promoted as a means of protecting personal privacy, free speech and human rights and avoiding personal data misuse.

- ***Proxy services*** protect users' privacy by having a third-party register the name. The third-party is most often the proxy service itself. The third-party allows the user to access and use the domain name through a separate agreement or some other arrangement directly with the user. Proxy service providers may include web design, law, and marketing firms; web hosts, registrar subsidiaries, resellers and individuals.

NOTE: The 2013 Registrar Accreditation Agreement contains a temporary specification relating to Privacy & Proxy Services (http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.pdf), which refers to these services as follows:

> 1.1 "P/P Customer" means, regardless of the terminology used by the P/P Provider, the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.
>
> 1.2 "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services.
>
> 1.3 "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration

Data Service (WHOIS) or equivalent services rather than the P/P Customer's contact information.

1.4 "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including Registrar and its Affiliates, as applicable.

(2) Relay & Reveal Requests

The following descriptions are taken from the GNSO's Terms of Reference for a proposed Proxy & Privacy Relay & Reveal Study in 2010 (http://gnso.icann.org/issues/whois/whois-proxy-privacy-relay-reveal-studies-tor-29sep10-en.pdf):

- For many domains, Registered Name Holders can be reached directly at addresses obtained from WHOIS. However, for Privacy/Proxy-registered domains, Registered Name Holders or third party licensees cannot be reached directly via WHOIS- published addresses. Instead, ***communication relay requests*** may be sent to the Privacy/Proxy service provider published in WHOIS, or attempted using addresses obtained from other sources, websites or communications associated with the domain.

- For many domains (including those registered via Privacy services), the Registered Name Holder's identity is published directly in WHOIS. However, for domains registered via Proxy services, the name of the licensee is not published in WHOIS; third party licensees can typically only be identified by ***asking the Proxy to reveal the licensee's identity***, given reasonable evidence of actionable harm.

Annex C – Request for Input from other ICANN SO / ACs

Dear SO/AC Chair,

As you may be aware, the GNSO Council recently initiated a Policy Development Process (PDP) on Privacy & Proxy Services Accreditation Issues. As part of its efforts to obtain input from the broader ICANN Community at an early stage of its deliberations, the Working Group that has begun to explore questions related to these issues is looking for any input or information that may help inform our deliberations.

Below you will find an overview of the issues that the WG has been assigned to address in its charter. We would appreciate it very much if you would examine the items and provide any input that your group may have to the GNSO Secretariat (gnso.secretariat@gnso.icann.org) by **Friday 28 February 2014**. If you cannot submit your input by that date, but your group would like to contribute, please let us know when we can expect to receive your contribution so that we can plan accordingly. While we would like your thoughts on all items, responses to a subset still will be helpful. Please feel free also to suggest modifications to or additional questions that your group believes useful for the WG to address.

Your input will be valuable for informing the WG as we begin our work. We have included a list of relevant definitions at the end of this document in the hope that they will be of assistance to your group in providing input. For further background information on our WG's activities to date and to follow our work as we move forward, see https://community.icann.org/x/9iCfAg.

With best regards,

Don Blumenthal, Chair of the Privacy & Proxy Services Accreditation Issues PDP Working Group

QUESTIONS FOR WHICH THE WG WAS CHARTERED AND IS SEEKING INPUT

This RAA PDP Working Group (WG) was created to provide the GNSO Council with policy recommendations regarding the issues identified during the 2013 RAA negotiations, including recommendations made by law enforcement and GNSO working groups, that were not addressed during the 2013 RAA negotiations but are otherwise suited for a PDP. These issues focus on the accreditation of Privacy & Proxy Services.

As part of its deliberations on the matter, the RAA PDP WG was asked to, at a minimum, consider those issues detailed in the Staff Briefing Paper published on 16 September 2013 and included in the WG Charter (see https://community.icann.org/display/gnsopnpsrvaccrdtwg/WG+Charter). The WG has organized the questions in the hope that it adds clarity.

I. MAIN ISSUES

7. What, if any, are the types of Standard Service Practices that should be adopted and published by ICANN-accredited privacy/proxy service providers?
8. Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?
9. What are the contractual obligations, if any, that if unfulfilled would justify termination of customer access by ICANN-accredited privacy/proxy service providers?
10. What types of services should be covered, and would be the forms of non-compliance that would trigger cancellation or suspension of registrations?
11. What are the effects of the privacy and proxy service specification contained in the 2013 RAA? Have these new requirements improved WHOIS quality, registrant contactability and service usability?
12. What should be the contractual obligations of ICANN accredited registrars with regard to accredited privacy/proxy service providers? Should registrars be permitted to knowingly accept registrations where the registrant is using unaccredited service providers that are however bound to the same standards as accredited service providers?

II. MAINTENANCE

7. Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made through a privacy/proxy service?
8. Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?
9. What rights and responsibilities should customers of privacy/proxy services have? What obligations should ICANN-accredited privacy/proxy service providers have in managing these rights and responsibilities? Clarify how transfers, renewals, and PEDNR policies should apply.

10. Should ICANN-accredited privacy/proxy service providers distinguish between domain names used for commercial vs. personal purposes? Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes?
11. Should there be a difference in the data fields to be displayed if the domain name is registered or used for a commercial purpose, or by a commercial entity instead of a natural person?
12. Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?

III. CONTACT

1. What measures should be taken to ensure contactability and responsiveness of the providers?
2. Should ICANN-accredited privacy/proxy service providers be required to maintain dedicated points of contact for reporting abuse? If so, should the terms be consistent with the requirements applicable to registrars under Section 3.18 of the RAA?
3. Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?
4. What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?

IV. RELAY

3. What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers?
4. Should ICANN-accredited privacy/proxy service providers be required to forward to the customer all allegations of illegal activities they receive relating to specific domain names of the customer?

V. REVEAL

8. What, if any, are the baseline minimum standardized reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
9. Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for the specific purpose of ensuring timely service of cease and desist letters?
10. What forms of alleged malicious conduct, if any, and what evidentiary standard would be sufficient to trigger such disclosure? What specific alleged violations, if any, would be sufficient to trigger such publication?
11. What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?
12. What safeguards or remedies should be available in cases where publication is found to have been unwarranted?
13. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
14. What clear, workable, enforceable and standardized processes should be adopted by ICANN-

accredited privacy/proxy services in order to regulate such access (if such access is warranted)?

LIST OF RELEVANT DEFINITIONS

(3) Privacy & Proxy Services

The following definitions are those used by the GNSO in the various WHOIS studies it commissioned between 2010-2012 (http://gnso.icann.org/issues/whois/whois-working-definitions-study-terms-18feb09.pdf):

- ***Privacy services*** hide customer details from going into WHOIS. Privacy service providers, which may include registrars and resellers, may offer alternate contact information and mail forwarding services while not actually shielding the domain name registrant's identity. By shielding the user in these ways, these services are promoted as a means of protecting personal privacy, free speech and human rights and avoiding personal data misuse.

- ***Proxy services*** protect users' privacy by having a third-party register the name. The third-party is most often the proxy service itself. The third-party allows the user to access and use the domain name through a separate agreement or some other arrangement directly with the user. Proxy service providers may include web design, law, and marketing firms; web hosts, registrar subsidiaries, resellers and individuals.

NOTE: The 2013 Registrar Accreditation Agreement contains a temporary specification relating to Privacy & Proxy Services, which refers to these services as follows (http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.pdf):

> 1.1 "P/P Customer" means, regardless of the terminology used by the P/P Provider, the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.
>
> 1.2 "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services.
>
> 1.3 "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (WHOIS) or equivalent services rather than the P/P Customer's contact information.

1.4 "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including Registrar and its Affiliates, as applicable.

(4) Relay & Reveal Requests

The following descriptions are taken from the GNSO's Terms of Reference for a proposed Proxy & Privacy Relay & Reveal Study in 2010 (http://gnso.icann.org/issues/whois/whois-proxy-privacy-relay-reveal-studies-tor-29sep10-en.pdf):

- For many domains, Registered Name Holders can be reached directly at addresses obtained from WHOIS. However, for Privacy/Proxy-registered domains, Registered Name Holders or third party licensees cannot be reached directly via WHOIS- published addresses. Instead, ***communication relay requests*** may be sent to the Privacy/Proxy service provider published in WHOIS, or attempted using addresses obtained from other sources, websites or communications associated with the domain.

- For many domains (including those registered via Privacy services), the Registered Name Holder's identity is published directly in WHOIS. However, for domains registered via Proxy services, the name of the licensee is not published in WHOIS; third party licensees can typically only be identified by ***asking the Proxy to reveal the licensee's identity***, given reasonable evidence of actionable harm.

Annex D – 2013 RAA Interim Privacy / Proxy Specification