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

STATUS OF THIS DOCUMENT

This is the Final Report on Privacy & Proxy Services Accreditation Issues, prepared by ICANN staff and the Working Group for submission to the GNSO Council on 7 December 2015.

SUMMARY

This report is submitted to the GNSO Council for its consideration 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 existing rights protection mechanisms, is the subject of a Preliminary Issue Report that was published for public comment in October 2015[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]. The 2013

[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/issues/new-gtlds/rpm-prelim-issue-09oct15-en.pdf. Note that where the original Council resolution (http://gnso.icann.org/en/council/resolutions#201112) had called for the Issue Report to be published 18 months after the delegation of the first gTLD in the New gTLD Program, an extension of the deadline to October 2015 was approved by the Council in January 2015: http://gnso.icann.org/en/meetings/minutes-council-29jan15-en.htm.

[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.

RAA also contemplates the development and implementation of a privacy and proxy service accreditation by ICANN[6].

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 Working Group ("WG") was issued on 6 November 2013, and the WG held its first meeting on 3 December 2013[7]. On 5 May 2015, the WG published its Initial Report for public comment[8].

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 WG conducted by conference call as well as via its mailing list 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 that were presented for public comment in its Initial Report. To prepare this Final Report, the WG used a uniform Public Comment Review Tool to facilitate its analysis of the community input received on its Initial Report, and formed four Sub Teams to review specific categories of public comments received.

The WG's findings and final recommendations for all of its Charter questions can be found in full in Section 7 of this Final Report. They are also summarized in Section 1.3 below.

---

[6] See, e.g., Section 3.14 of the 2013 RAA: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa.

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

[8] The Initial Report, public comments received and the staff report of the public comments can be viewed at https://www.icann.org/public-comments/ppsai-initial-2015-05-05-en.

1.3 The Working Group's Final 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". When it published its Initial Report, the WG had agreed on a set of preliminary conclusions for most of its Charter questions, although in several instances it had not yet finalized an agreed position on particular issues. This Final Report contains all the WG's consensus recommendations on all its Charter questions, based on further WG deliberations and its review of the public comments it received to the Initial Report.

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[9].

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

1.3.1 Summary of the WG's final consensus recommendations

In finalizing its recommendations, the WG noted at several points during its deliberations that there are likely to be implementation challenges in applying accreditation standards to privacy and proxy service providers who are not affiliated with an ICANN-accredited registrar. The WG identified a number of

[9] 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.

topics amongst its Charter questions that might raise these types of challenges. These include the impact of a transfer of a domain name registration on privacy or proxy services to a customer, the effect on a customer of de-accreditation of a privacy or proxy service provider, and the option for a privacy or proxy service provider to offer cancellation of a domain name registration in lieu of disclosure of customer information in response to a valid third party request. While the WG believes that the accreditation policies it is recommending are adequate to address most of these situations, it also recognizes that the implementation of these policies in the case of accredited service providers that are not affiliated with ICANN-accredited registrars may require implementation adjustment.

The WG has reached **FULL CONSENSUS** on all the following recommendations:

I. DEFINITIONS:

1. The WG recommends the adoption of the following definitions, to avoid ambiguities surrounding the common use of certain words in the WHOIS context. The WG recommends that these recommendations be used uniformly by ICANN, including generally in relation to WHOIS beyond privacy and proxy service issues:

   - ***"Privacy Service"*** means 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 privacy or proxy service provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services[10].
   - ***"Proxy Service"*** is a service through which a Registered Name Holder licenses use of a Registered Name to the privacy or proxy customer in order to provide the privacy or proxy customer use of the domain name, and the Registered Name Holder's contact information is

[10] The definitions of Privacy Service and Proxy Service reflect those in the 2013 RAA. In this context, the 2013 RAA also defines "Registered Name" as a domain name within the domain of a gTLD, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance, and "Registered Name Holder" is defined as the holder of a Registered Name.

displayed in the Registration Data Service (WHOIS) or equivalent services rather than the customer's contact information.

NOTE: In relation to the definitions of a Privacy Service and a Proxy Service, the WG makes the following additional recommendation:

- Registrars are not to knowingly[11] accept registrations from privacy or proxy service providers who are not accredited through the process developed by ICANN. For non-accredited entities registering names on behalf of third parties, the WG notes that the obligations for Registered Name Holders as outlined in section 3.7.7 of the 2013 RAA would apply[12].

- ***"Affiliate"***, when used in this Final Report in the context of the relationship between a privacy or proxy service provider and an ICANN-accredited registrar, means a privacy or proxy service provider that is Affiliated with such a registrar, in the sense that word is used in the 2013 RAA. Section 1.3 of the 2013 RAA defines an "Affiliate" as a person or entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, the person or entity specified.
- ***"Publication"*** means the reveal[13] of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details in the WHOIS system.

[11] In this context, "knowingly" refers to actual knowledge at the time that the registration is submitted to the registrar. As implementation guidance, this knowledge would normally be obtained through a report to the registrar from ICANN or a third party.
[12] Section 3.7.7.3 of the 2013 RAA reads as follows: "Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name."
[13] As the single word "reveal" has been used in the WHOIS context to describe the two distinct actions that the WG has defined as "Disclosure" and "Publication", the WG is using "reveal" within its definitions as part of a more exact description, to clarify which of the two meanings would apply in any specific instance. The rest of this Initial Report generally uses the terms "Disclosure" and "Publication" to refer to the relevant specific aspect of a "reveal".

- ***"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 Requester 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 privacy or proxy service provider is established or maintains a physical office. This definition is based on Section 3.18.2 of the 2013 Registrar Accreditation Agreement, which provision spells out a registrar's obligation to maintain a point of contact for, and to review reports received from, law enforcement authorities[14]; as such, the WG notes that its recommendation for a definition of "law enforcement authority" in the context of privacy and proxy service accreditation should also be updated to the extent that, and if and when, the corresponding definition in the RAA is modified.
- ***"Relay"***, when used in the context of a request to a privacy or proxy service provider from a Requester, means to forward the request to, or otherwise notify, the privacy or proxy service customer that a Requester is attempting to contact the customer.
- ***"Requester"***, when used in the context of Relay, Disclosure or Publication, including in the Illustrative Disclosure Framework described in Annex B, means an individual, organization or entity (or its authorized representatives) that requests from a privacy or proxy service provider either a Relay, or Disclosure or Publication of the identity or contact details of a customer, as the case may be.

II. NO DISTINCTION IN TREATMENT; WHOIS LABELING REQUIREMENTS; VALIDATION & VERIFICATION OF CUSTOMER DATA:

2. Privacy and proxy services ("P/P services") are to be treated the same way for the purpose of the accreditation process.

[14] See https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

3. The status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether P/P 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, P/P registrations should not be limited to private individuals who use their domains for non-commercial purposes.

4. To the extent that this is feasible, domain name registrations involving P/P service providers should be clearly labelled as such in WHOIS[15].

5. P/P customer data is to be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Program Specification of the 2013 RAA (as may be updated from time to time). In the cases where a P/P service provider is Affiliated with a registrar and that Affiliated registrar has carried out validation and verification of the P/P customer data, re-verification by the P/P service provider of the same, identical, information should not be required.

MANDATORY PROVISIONS TO BE INCLUDED IN PROVIDER TERMS OF SERVICE & MINIMUM REQUIREMENTS TO BE COMMUNICATED TO CUSTOMERS:

6. All rights, responsibilities and obligations of registrants and P/P service customers as well as those of accredited P/P service providers need to be clearly communicated in the P/P service registration agreement, including a provider's obligations in managing those rights and responsibilities and any specific requirements applying to transfers and renewals of a domain name. In particular, all accredited P/P service providers 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.

[15] While this may be possible with existing fields, the WG has also explored the idea that the label might also be implemented by adding another field to WHOIS, and is aware that this may raise certain questions that should be appropriately considered as part of implementation. For clarity, references to "WHOIS" in this Final Report are to the current globally accessible gTLD Registration Directory Service as well as any successors or replacements thereto.

7. All accredited P/P service providers must include on their websites, and in all Publication and Disclosure-related policies and documents, a link to either a request form containing a set of specific, minimum, mandatory criteria, or an equivalent list of such criteria, that the provider requires in order to determine whether or not to comply with third party requests, such as for the Disclosure or Publication of customer identity or contact details.

8. All accredited P/P service providers must publish their terms of service, including pricing (e.g. on their websites). In addition to other mandatory provisions recommended by the WG, the terms should at a minimum include the following elements in relation to Disclosure and Publication:

   - Clarification of when those terms refer to Publication requests (and their consequences) and when they refer 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, including Publication in the event of a customer's initiation of a transfer of the underlying domain name[16]. In making this recommendation, the WG noted the changes to be introduced to the Inter Registrar Transfer Policy ("IRTP") in 2016, where following a Change of Registrant[17] a registrar is required to impose a 60-day inter-registrar transfer lock.
   - Clarification as to whether or not a customer: (1) will be notified when a provider receives a Publication or Disclosure request from a third party; and (2) may opt to cancel its domain registration prior to and in lieu of Publication or Disclosure. However, accredited P/P service providers that offer this option should nevertheless expressly prohibit cancellation of a domain name that is the subject of a UDRP proceeding.

[16] The WG believes there should be no mandatory restriction on providers being able to terminate service to a customer on grounds stated in the terms of service, subject to any other specific limitation that may be recommended in this report by the WG. The WG notes that it is probably not possible to create a general policy that would in all cases prevent Publication via termination of service where the customer is ultimately shown to have been innocent (i.e. not in breach).

[17] This is defined as a material, i.e. non-typographical, change to either the registrant name, organization or email address (or in the absence of an email contact, the administrative contact listed for the registrant).

- Clarification that a Requester 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.

9. In addition, the WG recommends the following as best practices for accredited P/P service providers[18]:

- P/P service providers should facilitate and not obstruct the transfer[19], renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the Expired Registration Recovery Policy and transfers to another registrar.
- P/P service providers 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.
- P/P service providers should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved online location such as the provider's own website) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication.

CONTACTABILITY & RESPONSIVENESS OF PRIVACY & PROXY SERVICE PROVIDERS:

10. ICANN should publish and maintain a publicly accessible list of all accredited P/P service providers, with all appropriate contact information. Registrars should be advised to provide a web link to P/P services run by them or their Affiliates as a best practice. P/P service providers

[18] The WG recognizes that implementation of these recommendations may involve the development of new procedures.
[19] See also the WG's observations below under Recommendation #21 regarding the additional risks and challenges that may arise when the P/P service provider is independent of (i.e. not Affiliated with) an ICANN-accredited registrar, and which may be of particular concern in relation to transfers and de-accreditation issues.

should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program[20].

11. P/P service providers must maintain a point of contact for abuse reporting purposes. In this regard, a "designated" rather than a "dedicated" point of contact will be sufficient, since the primary concern is to have one contact point that third parties can go to and expect a response from. For clarification, the WG notes that as long as the requirement for a single point of contact can be fulfilled operationally, it is not mandating that a provider designate a specific individual to handle such reports.

12. P/P service providers should be fully contactable, through the publication of contact details on their websites in a manner modelled after Section 2.3 of the 2013 RAA Specification on Privacy and Proxy Registrations, as may be updated from time to time.

13. Requirements relating to the forms of alleged malicious conduct to be covered by the designated published point of contact at an ICANN-accredited P/P 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[21] in the New gTLD Registry Agreement or Safeguard 2, Annex 1 of the GAC's Beijing Communique[22] could serve as starting points for developing such a list.

---

[20] The WG discussed, but did not reach consensus on, the possibility of requiring a registrar to also declare its Affiliation (if any) with a P/P service provider.

[21] 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."

[22] 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."

14. The designated point of contact for a P/P service provider should be capable and authorized to investigate and handle abuse reports and information requests received.

STANDARD FORM & REQUIREMENTS FOR ABUSE REPORTING & INFORMATION REQUESTS:

15. A uniform set of minimum mandatory criteria that must be followed for the purpose of reporting abuse and submitting requests (including requests for the Disclosure of customer information) should be developed. Forms that may be required by individual P/P service providers for this purpose should also include space for free form text[23]. P/P service providers should also have the ability to "categorize" reports received, in order to facilitate responsiveness. P/P service providers must also state the applicable jurisdiction in which disputes (including any arising under the Illustrative Disclosure Framework in Annex B) should be resolved on any forms used for reporting and requesting purposes.

RELAYING (FORWARDING) OF THIRD PARTY REQUESTS:

16. Regarding Relaying of Electronic Communications[24]:

- All communications required by the RAA and ICANN Consensus Policies must be Relayed.
- For all other electronic communications, P/P service providers may elect one of the following two options:
    i. Option #1: Relay all electronic requests received (including those received via 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

[23] With the specific exception of Disclosure requests from intellectual property rights holders (see Recommendation #19 below), the WG discussed but did not finalize the minimum elements that should be included in such a form in relation to other requests and reports. The WG notes that this recommendation is not intended to prescribe the method by which a provider should make this form available (e.g. through a web-based form) as providers should have the ability to determine the most appropriate method for doing so.

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

ii. Option #2: Relay all electronic requests received (including those received via emails and web forms) from law enforcement authorities and third parties containing allegations of domain name abuse (i.e. illegal activity)

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

17. 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 service customer will be promptly Relayed to the customer. A Requester will be promptly notified of a persistent failure of delivery[25] that a P/P service 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 in relation to a relay request 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 upon request Relay a further form of notice to its customer. A provider should have the discretion to select the most appropriate means of Relaying such a request. A provider shall have the right to impose reasonable limits on the number of such requests made by the same Requester for the same domain name.
- When a service provider becomes aware of a persistent delivery failure to a customer as described herein, that will trigger the P/P service provider's obligation to perform a verification/re-verification (as applicable) of the customer's email address(es), in accordance

[25] 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.

with the WG's recommendation that customer data be validated and verified in a manner consistent with the WHOIS Accuracy Specification of the 2013 RAA (see the WG's Recommendation #5, above, and the background discussion under Category B, Question 2 in Section 7, below).

- However, these recommendations shall not preclude a P/P service 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.

DISCLOSURE OR PUBLICATION OF A CUSTOMER'S IDENTITY OR CONTACT DETAILS:

18. Regarding Disclosure and Publication, 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 P/P service providers to review requests manually or to facilitate direct resolution of an issue between a Requester and a P/P service 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. In relation to Publication that is subsequently discovered to be unwarranted, the WG believes that contractual agreements between providers and their customers and relevant applicable laws will govern, and are likely to provide sufficient remedies in such instances.

19. The WG has developed an illustrative Disclosure Framework to apply to Disclosure requests made to P/P service providers by intellectual property (i.e. trademark and copyright) owners. The proposal includes requirements concerning the nature and type of information to be provided by a Requester, non-exhaustive grounds for refusal of a request, and the possibility of neutral dispute resolution/appeal in the event of a dispute. The WG recommends that a review of this Disclosure Framework be conducted at an appropriate time after the launch of the program and periodically thereafter, to determine if the implemented recommendations meet the policy objectives for which they were developed. Such a review might be based on the non-exhaustive list of guiding principles developed by the GNSO's Data and Metrics for Policy Making (DMPM) WG, as adopted by the GNSO Council and ICANN Board. As noted by the DMPM WG, relevant metrics could include industry sources, community input via public comment or surveys

or studies. In terms of surveys (whether or providers, customers or requesters), data should be anonymized and aggregated. Please refer to Annex B for the full Disclosure Framework.

20. Although the WG has reached consensus on an illustrative Disclosure Framework for handling requests from intellectual property (i.e. trademark and copyright) rights-holders, it has not developed a similar framework or template that would apply to other Requesters, such as LEA or anti-abuse and consumer protection groups. The WG is aware that certain concerns, such as the need for confidentiality in relation to an on-going LEA investigation, may mean that different considerations would apply to any minimum requirements that might be developed for such a framework. In this regard, in its Initial Report the WG had sought community feedback on specific concerns relating to the handling of LEA requests, such as whether or not providers should be mandated to comply with them. Based on input received, the WG recommends that accredited P/P service providers should comply with express requests from LEA not to notify a customer where this is required by applicable law. However, this recommendation is not intended to prevent providers from either voluntarily adopting more stringent standards or from cooperating with LEA. In the event that a Disclosure Framework is eventually developed for LEA requests, the WG recommends that the Framework expressly include requirements under which at a minimum: (a) the Requester agrees to comply with all applicable data protection laws and to use any information disclosed to it solely for the purpose to determine whether further action on the issue is warranted, to contact the customer, or in a legal proceeding concerning the issue for which the request was made; and (b) exempts Disclosure where the customer has provided, or the P/P service provider has found, specific information, facts, and/or circumstances showing that Disclosure will endanger the safety of the customer.

DEACCREDITATION & ITS CONSEQUENCES:

21. Regarding de-accreditation of a P/P service provider:

The WG reiterates its previous observation that increased risks to a customer's privacy may be involved when a customer is dealing with a P/P service provider who, even if accredited by ICANN, is not Affiliated with an ICANN-accredited registrar. De-accreditation was noted as one topic where additional

problems may arise. The WG therefore recommends that the following general principles be adopted and followed when a more detailed P/P service de-accreditation process is developed during implementation. As with transfers of domain names that occur other than as a result of de-accreditation of a P/P service provider, these principles are based on the WG's belief that customer privacy should be a paramount concern. As such, reasonable safeguards to ensure that a customer's privacy is adequately protected in the course of de-accreditation of a customer's P/P service provider – including when transfer of a customer's domain name or names is involved – should be integral to the rules governing the de-accreditation process.

Principle 1: A P/P service customer should be notified in advance of de-accreditation of a P/P service provider. The WG notes that the current practice for registrar de-accreditation involves the sending of several breach notices by ICANN Compliance prior to the final step of terminating a registrar's accreditation. While P/P service provider de-accreditation may not work identically to that for registrars, the WG recommends that ICANN explore practicable ways in which customers may be notified during the breach notice process (or its equivalent) once ICANN issues a termination of accreditation notice but before the de-accreditation becomes effective. The WG recommends that de-accreditation become effective for existing customers 30 days after notice of termination. The WG notes that, in view of the legitimate need to protect many customers' privacy, the mere publication of a breach notice on the ICANN website (as is now done for registrar de-accreditation) may not be sufficient to constitute notice.

Principle 2: Each step in the de-accreditation process should be designed so as to minimize the risk that a customer's personally identifiable information is made public.

Principle 3: The WG notes that the risk of inadvertent publication of a customer's details in the course of de-accreditation may be higher when the provider in question is not Affiliated with an ICANN-accredited registrar. As such, implementation design of the de-accreditation process should take into account the different scenarios that can arise when the provider being de-accredited is, or is not, Affiliated with an ICANN-accredited registrar.

In addition to the three principles outlined above, the WG recommends specifically that, where a Change of Registrant (as defined under the IRTP) takes place during the process of de-accreditation of a

proxy service provider, a registrar should lift the mandatory 60-day lock at the express request of the beneficial user, provided the registrar has also been notified of the de-accreditation of the proxy service provider[26].

1.3.2. ADDITIONAL GENERAL RECOMMENDATIONS

In addition to the recommendations it developed for each of its Charter questions, the WG also recommends that the following general principles be adopted as part of the P/P service provider accreditation program.

First, the next review of the IRTP should include an analysis of the impact on P/P service customers, to ensure that adequate safeguards are in place as regards P/P service protection when domain names are transferred pursuant to an IRTP process. Where a P/P service customer initiates a transfer of a domain name, the WG recognizes that a registrar should have the same flexibility that it has currently to reject incoming transfers from any individual or entity, including those initiated by accredited P/P services. Nevertheless, the WG recommends that, in implementing those elements of the P/P service accreditation program that pertain to or that affect domain name transfers and in addition to its specific recommendations contained in this Final Report, ICANN should perform a general "compatibility check" of each proposed implementation mechanism with the then-current IRTP.

Secondly, the WG recommends that ICANN develop a public outreach and educational program for registrars, P/P service providers and customers (including potential customers) to inform them of the existence, launch and features of the P/P service accreditation program.

Thirdly, the WG recommends that providers should be required to maintain statistics on the number of Publication and Disclosure requests received and the number honored, and provide these statistics in aggregate form to ICANN for periodic publication. The data should be aggregated so as not to create a market where nefarious users of the domain name system are able to use the information to find the P/P service that is least likely to make Disclosures.

[26] The WG notes that the new changes to the IRTP give a registrar the discretion to lift the lock at the beneficial user's request, and that no specific exceptions were created at the time the policy was reviewed.

Finally, the WG has concluded that the registrar accreditation 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. The implications of adopting a particular accreditation model will need to be worked out as part of the implementation of its policy recommendations, if adopted.

1.3.3. ADDITIONAL NOTE ON OPEN ISSUES IN THE INITIAL REPORT CONCERNING DOMAIN NAMES ACTIVELY USED FOR COMMERCIAL TRANSACTIONS

As noted in the Initial Report, the WG was unable at the time to achieve consensus on the important question of "whether domain names that are actively used for commercial transactions should be prohibited from using P/P services." In contrast to many other questions on which the WG was able to reach provisional conclusions, the split of views on this question[27] was sufficiently intractable that it was decided to pose three questions to the public during the public comment period for the Initial Report.[28]

The first question asked whether "registrants of domain names associated with commercial activities and which are used for online financial transactions [should] be prohibited from using, or continuing to use, P/P services." Responses to the two remaining questions were contingent on support for a positive response to the first question, i.e., a viewpoint that such registrants should no longer be allowed to use P/P services ("If you agree with this position [the prohibition], do you think it would be useful to adopt a definition of commercial or transactional to define those domains for which p/p service registration should be disallowed? If so, what should the definitions be?")

A WG Sub-Team analyzed the thousands of comments received that either directly responded to the first question posed, or that appeared to the Sub Team to be highly relevant to it (such as the many comments that endorsed statements that support *"the use of privacy services by all, for all legal purposes, regardless of whether the website is "commercial")."* Numerically, an overwhelming majority

[27] See Annex F of the Initial Report for statements from WG members setting out the contrasting views. See also pp. 48-49 of the Initial Report for summaries of the opposing views.
[28] Notably, this issue is the only one characterized in the Initial Report as a "specific topic on which there is currently no consensus within the WG"; see the Initial Report at p.15.

of these comments answered the question posed in the negative and supported no restrictions on the use of P/P services.

Several commenters, representing significant groups of stakeholders, noted that a yes-or-no response to the question posed was difficult because the WG did not present an agreed-upon definition of terms such as "commercial activities" or "online financial transactions." In other words, it is difficult to assume that the many commenters who answered (in effect) that registrations used to engage in "commercial activities" or to carry out "online financial transactions" should continue to be allowed to use P/P services would necessarily have answered the question the same way with regard to all conceivable definitions of these terms. This point is well taken, and perhaps the public sentiment would have been different had an agreed-upon definition been supplied as part of the first question. On the other hand, according to the Sub-Team's analysis of responses to Question 2, in which the public was asked to propose definitions of "commercial" and "transactional," but only if they agreed with the concept of introducing a prohibition on use of P/P services for such purposes, many such respondents believe that defining commercial and transactional will be difficult at best, and some believe it to be impossible[29].

In fact the question was not posed in the context of an agreed definition of these terms, and the WG's job following the public comment period was to analyze and draw conclusions from the answers provided to the questions asked. This analysis took place in the context of a status quo in which there are no restrictions on uses to which domain names registered using these services may be put.

Under these circumstances, the WG does not believe that the accreditation standards for P/P services should require service providers to differentiate between registrants who wish to use these services to engage in commercial activities or online financial transactions and registrants who do not. This conclusion seeks to reflect the clear majority of opinions expressed in the comments, but also rests on pragmatic grounds: because it will certainly be difficult (at best) to achieve a consensus definition of critical terms that must be defined in order to incorporate this principle into accreditation standards, the

[29] The Working Group acknowledges that because (as noted below) some services currently impose restrictions on commercial uses of proxy registrations, making the needed definitions and distinctions is apparently possible, but seeks to fairly represent the sentiments of the public comment by including that statement here.

WG does not support delaying the adoption and implementation of an accreditation system until such a consensus can be reached.

The WG notes that at least some significant current providers of these services have adopted and do enforce similar restrictions on who may use their particular services. The WG's conclusion that such a prohibition should not be incorporated into accreditation standards at this time is not meant to discourage accredited providers from adopting and implementing such policies if they so choose (provided that other relevant criteria, such as publication of terms of service and grounds for termination of the service, are fulfilled). The WG also notes that at least some registrants engaged in commercial transactions using domain names registered through P/P services are doing so to carry out illegal activities or other abuses that may provide a basis for disclosure or publication under another part of these accreditation standard, or under terms of service adopted and published by accredited providers. In other words, the WG's conclusion that registrants engaged in commercial or transactional activities should not be considered per se ineligible to use P/P services should have no impact on a particular registrant's eligibility (or not) to do so on other grounds.

1.4 Public Comments on the Initial Report

A public comment forum was open upon publication of the WG's Initial Report on 5 May 2015. In response to the WG's request, the public comment period ran for sixty-three (63) days, closing on 7 July 2015. Due to the number and volume of comments received, which included well over 11,000 individual submissions (many of which were based on an online template), an online petition signed by over 10,000 persons (many of whom also submitted additional comments) and over 150 specific responses to an online template containing all the WG's preliminary recommendations[30], the WG extended its planned timeline to allow for full review of all the comments received. In view of the public's interest in the issue, the WG co-chairs also published a blog post explaining the public comment process and the WG's working procedures[31].

[30] All the individual submissions that were made directly to the public comment forum as well as the staff report of the public comments can be viewed here: https://www.icann.org/public-comments/ppsai-initial-2015-05-05-en. A summary of the individual responses to the WG's online question template as well as the template itself can be viewed here: https://community.icann.org/x/KIFCAw.
[31] See https://www.icann.org/news/blog/ppsai-wg-status-update-and-observations.

1.5 Conclusions and Next Steps

The WG recommends that the GNSO Council adopt all the consensus recommendations contained in this Final Report, following its satisfactory review of the WG's work and processes.

2. Objective and Next Steps

This Final Report on the Privacy and Proxy Services Accreditation Issues Policy Development Process ("PDP") was prepared as required by the GNSO Policy Development Process stated in the ICANN Bylaws, Annex A. This Final Report is based on the Initial Report of 5 May 2015, and has been updated to reflect the WG's review and analysis of the public comments received and its own further deliberations. This Report is being been submitted to the GNSO Council for its consideration. If the GNSO Council approves this Final Report, ICANN staff will prepare a GNSO Council Recommendations Report, which will be sent along with the Final Report to the ICANN Board. Following a public comment period, the ICANN Board will then make the determination whether to approve the policies recommended by the WG in this Final Report.

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. The agreement as approved contemplates the creation and implementation of a privacy and proxy service provider accreditation program by ICANN[32].
- On 16 September 2013, ICANN staff published a paper 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.

[32] See Section 3.14 of the 2013 RAA.

- 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 that could be considered as not having been addressed adequately: (1) clarification of registrar responsibilities in connection with proceedings under the existing UDRP[33]; and 2) privacy and proxy services – including accreditation and reveal/relay procedures.

With regard to P/P services, the 2013 RAA contains an interim specification[34] 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 applicable to privacy and proxy services offered by ICANN-accredited Registrars or their Affiliates, including those distributed through Resellers. 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 P/P 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

[33] 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.
[34] See https://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#privacy-proxy.

communications to a P/P 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 protections that can be put in place for accredited P/P service 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[35].

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 P/P 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 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[36], 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 the terms "privacy service" and "proxy service") that were used to frame the GNSO's WHOIS studies.

3.2.3 Recommendations from the WHOIS Policy Review Team

[35] 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.

[36] 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[37] in May 2012. The Final Report had highlighted the lack of clear and consistent rules regarding P/P 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 labelling 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;

[37] 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 registration 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 P/P services[38]. 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 Requesters and providers
- Unmasking the identity of the underlying customer and publishing his/her name and contact details in WHOIS
- Requesters 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

[38] 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 P/P service providers in general, and offered the following additional specific recommendations[39]:

- 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 service providers must provide the Registrar with accurate and reliable contact details for all mandatory Purpose-Based Contacts[40], in order to reach the provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Registrant
- Accredited service providers 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

[39] See Recommended Principles 138-149 from Section VII and Annex H of the EWG Final Report.
[40] 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 conduct 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. As of 18 November 2015, the WG had held 76 meetings, not including Sub Team meetings or its open community sessions at ICANN Public Meetings.

The WG also prepared a Work Plan, which was reviewed and updated 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, input from other ICANN SO/ACs, and 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, open issues 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 with remote participants) meeting at the ICANN Public Meeting in Los Angeles in October 2014, facilitated by a community facilitator with expertise on the topic. In preparing this Final Report, the WG was again selected by the GNSO Council to conduct a further face-to-face meeting (including remote participation for WG members who could not attend the session in person). This took place at the ICANN Public Meeting in Dublin in October 2015.

The WG received well over 11,000 individual submissions (many based on an online template circulated by a group of concerned persons) directly to the Public Comment Forum that was opened for its Initial Report in May 2015. This included an online petition that was signed by over 10,000 persons, many of whom also submitted additional comments. Over 150 individual responses were also received to an online template published by the WG and containing all its preliminary recommendations and open questions that the WG had posted for feedback. In order to ensure a fair and thorough review of the volume of input, the WG used a uniform Public Comment Review Tool template, divided into four different parts to take into account all the comments received. In addition, the WG formed four Sub Teams to consider more specifically the feedback received on all the open issues the WG had not reached consensus on in its Initial Report, as well as to review all general comments received on the topic of P/P service provider accreditation. Each Sub Team had its own collaborative online workspace where all its working drafts were uploaded, and all Sub Team calls were recorded and transcribed[41].

4.2 Members of the Working Group

The members of the PPSAI WG are:

NCSG	Affiliation*	Attended**
Amr Elsadr	NCUC	21
David Cake	NCSG	36
Maria Farrell++	NCUC	13
Marie-Laure Lemineur++	NPOC	11
Roy Balleste	NCUC	17
Stephanie Perrin	NCUC	54
Wendy Seltzer	NCUC	1
Howard Fellman	NCUC	0
Kathy Kleiman	NCSG	70
James Gannon	NCSG	15

[41] The WG's Public Comment Review Tools can be viewed here: https://community.icann.org/x/KIFCAw, and the membership, meetings and work of all the Sub Teams can be viewed at each of their respective wiki pages on the WG's community workspace: https://community.icann.org/x/9iCfAg.

Rudi Vansnick	NPOC	8

CSG

Adamou Nacer	ISPCP	1
Alex Deacon	IPC	57
Hector Ariel Manoff	IPC	1
Brian Winterfeldt	IPC	3
Keith Kupferschmid	IPC	17
Kiran Malancharuvil	IPC	32
Kristina Rosette++	IPC	32
Steve Metalitz	IPC	78
Osvaldo Novoa	ISPCP	48
Philip Marano	IPC	36
Todd Williams	IPC	60
Victoria Sheckler	IPC	35
Griffin Barnett	IPC	65
Valeriya Sherman	IPC	67
David Hughes	IPC	27
Paul McGrady	IPC	50
Jim Bikoff	IPC	48
David Heasley	IPC	51
Don Moody	IPC	10
Emily Emanual	BC	4
Michael Adeyeye	BC	0
Justin Macy	BC	53
John Horton	BC	9
Libby Baney	BC	25
Michael Shoukry	BC	1
Christian Dawson	ISPCP	29
Laura Jedeed	BC	9
Katherine McGowan++	BC	0

Susan Kawaguchi	BC	43
Chris Chaplow	BC	1
Phil Corwin	BC	37
Terri Stumme	BC	21
Sean McInerney	IPC	6
Seth Arnold	IPC	0

RrSG

Ben Anderson	4
Jeffrey Eckhaus	0
Gordon Dick	5
Graeme Bunton	69
Tatiana Khramtsova	44
James Bladel	59
Luc Seufer	53
Matt Serlin	2
Michele Neylon	48
Nicolas Steinbach	6
Rob Villeneuve	0
Tobias Sattler	15
Susan Prosser	32
Tim Ruiz++	22
Volker Greimann	61
Theo Geurts	17
Sarah Wyld	57
Darcy Southwell	60
Billy Watnpaugh	3
Jennifer Standiford	12
Chris Pelling	52
Bob Wiegand	0
Lindsay Hamilton-Reid	23

Ivens Oliveira Porto		0
Roger Carney		17
Sara Bockey		15
RySG		
Michael Palage		6
Statton Hammock		4
Bret Fausett		1
At Large/ALAC		
Carlton Samuels		47
Holly Raiche		45
Individuals		
Don Blumenthal		52
Eric Brunner-Williams		1
Dan Burke++		3
Frank Michlick		38
William Lin		0
Thomas Rickert		2
Other		
Gema Maria Campillos++	GAC	8
Richard Leaning++		12

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 18 November 2015. 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 representing the entirety of the deliberations of the WG.

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*[42]. 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, in accordance with the GNSO's PDP Manual.

5.2 Main Issues (Charter Questions Grouping Category A)

[42] 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.

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 had agreed early on that a useful and data-driven discussion of Question A-3 should only take place later on, given that the 2013 RAA only went into effect on 1 January 2014. The WG also considered that Questions A-1 or A-4 were general questions that would be better addressed following the WG's finalization of recommendations in the other Charter question categories. The WG's responses to these two questions therefore form part of its responses to other Charter questions, and as such are recorded

in those respective sections of this report. The WG's final recommendations 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 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[43] that the WG consider generally mandating the relay of ICANN-critical communications (such as required notices and reminders – for example, annual reminders under the WHOIS Data Reminder Policy and notices under the Expired Registration Recovery Policy). For transfers from a failed or de-accredited registrar, the Sub-Team considered that the situation would be almost fully covered by the IRTP.

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

In analysing the interplay between privacy protections (via use of a P/P 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

A. No P/P service involvement, (status quo under current IRTP)
B. Losing registrar has affiliated P/P, Gaining does not.
C. Gaining registrar has affiliated P/P, Losing does not.
D. 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 P/P services to exchange protected contact data, such as a hash function, in order to provide additional protection for the transfer of the domain name. In preparing its Final Report, the WG took into account the Sub-Team's work and deliberated issues that could arise which would impact the availability and use of privacy and proxy services in the event of a transfer of a domain name under the IRTP.

The WG's final recommendations 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?[44]

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[45] 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" purposes, uses and organizations. Concern was also expressed over whether enquiring into the "use" of

[44] 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.
[45] 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.

a domain name might implicate content issues. The WG's Initial Report contained two views on this question, for which public comment was solicited to assist the WG in developing its final recommendations. This Final Report represents the WG's consensus on this question following its review of the public comments received.

The WG's final recommendations 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[46]?

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

   b) Any difference if Requester is law enforcement vs. private party; if Requester 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 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

[46] 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.

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 final recommendations 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 Requester 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 P/P 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[47].

The GNSO Council therefore commissioned a feasibility survey that was conducted by the Interisle Consulting Group. The survey findings, published in August 2012, suggest 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 trade off 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 P/P 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.
By the time it published its Initial Report, the WG had come to agreement preliminarily regarding the relaying (or forwarding) by a P/P service provider of electronic communications. In dealing with the possibility that a third party Requester 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

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

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 P/P service provider action on 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 who offer P/P 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 P/P service provider's obligation to act in the event that a Requester 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[48]. The WG sought community feedback on both its agreed preliminary conclusions and the open issues on escalation on which there was no consensus at the time.
The WG's final recommendations 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.

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 Requester 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,

[48] See the WG's discussions on this point, under Charter Category Questions B-2 and B-3 (Section 7, below).

notwithstanding access to data by legitimate Requesters. 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 Requester?

g) What are the minimum standards of proof that should be required for the allegations being raised by the Requester?

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 Requester 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 Requester is law enforcement vs. private party; if Requester 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 Requester is law enforcement vs. private party; if Requester 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 P/P service provider Discloses – either to a specific third party Requester 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 Requester as opposed to Publication to the world at large. It reviewed a sampling of responses from various P/P 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 and their Affiliates who offer P/P 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 P/P service 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[49] its service to a customer as a result of that customer's breach of the terms of service.

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 Requesters – for example, 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 Requester, or both. The WG has developed an illustrative Disclosure framework for requests made by trademark and copyright owners or their authorized representatives (see Annex B). It has not, however, developed a similar framework for LEA and other types of third party Requesters.

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

The WG's final recommendations on this Category F can be found in Section 7.

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

[49] See further Section 5.8 below.

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 P/P service provider terminates service to a customer, as well as where the provider's accreditation is itself terminated by ICANN, i.e. de-accreditation.

The WG 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 need to 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. Following its review of the public comments received, the WG also sought guidance from the Registrar Services team on the operation and implications for P/P services of pending changes to the IRTP and, more generally, on how the WG might craft its final recommendations to ensure that safeguarding a P/P service customer's privacy remains a prime objective.

The WG's final recommendations for this Category G can be found in Section 7.

6. Community Input and Public Comments

6.1 Request for Input and Public Comments

According to the GNSO's PDP Manual[50], 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 SOs and ACs as well as GNSO Stakeholder Groups and Constituencies with a request for input 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.

The WG published its Initial Report – containing twenty preliminary recommendations and several open questions on which it had yet to reach consensus – for public comment on 5 May 2015. At the close of the sixty-three (63) day public comment period for its Initial Report, the WG had received well over 11,000 individual submissions (many based on an email template) to the public comment forum, including an online petition signed by over 10,000 persons, many of whom also appended additional individual statements. In addition, over 150 responses were received to the WG's online template containing all its preliminary recommendations and open questions, which the WG had posted to facilitate the provision of additional input. All the ICANN SO/ACs and GNSO Stakeholder Groups and Constituencies that had provided input in response to the WG's early solicitation of feedback also submitted public comments to the WG's Initial Report.

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

6.2 Review of Input Received

To facilitate its review of all the public comments, the WG used a uniform Public Comment Review Tool, which grouped the relevant comments into lists corresponding to the appropriate preliminary recommendation (as numbered and published in the WG's Initial Report). As the Initial Report contained twenty (20) preliminary recommendations (some with sub-parts) and several open issues, the Public Comment Review Tool was split into four distinct parts. In addition, four Sub-Teams of volunteer WG members were formed – three to consider the public comments related to the open issues noted in the Initial Report, and the fourth to review the remaining general comments that were placed into Part 4 of the Public Comment Review Tool. The WG also amended and extended its timeline under its Work Plan to accommodate its review of all the comments received.

The four parts of the WG's Public Comment Review Tool and the various initial review tools developed for each Sub Team based on the WG's template can be viewed at https://community.icann.org/x/KIFCAw. All working drafts and meetings of the four Sub-Teams were recorded and can be viewed at each Sub-Team's wiki page at https://community.icann.org/x/BI-hAg. The staff report of the public comments received can be viewed at https://www.icann.org/public-comments/ppsai-initial-2015-05-05-en#summary.

In addition to its weekly meetings and email discussions, the WG also conducted a second face-to-face meeting in Dublin in October 2015 (immediately prior to the ICANN Public Meeting), to continue its deliberations in preparation for this Final Report, based on its analysis of the public comments.

As a result of reviewing the input it received, the WG has refined and updated certain of its recommendations that were in its Initial Report. In further discussions following analysis of the relevant public comments, the WG has also come to agreement on the various open issues on which there had not been consensus at the time of the publication of its Initial Report. The final recommendations in this Final Report are therefore the result of the WG's considered discussions and incorporation, where relevant, of the community feedback provided to it.

7. Working Group Final Recommendations

7.1 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 final recommendations from the WG, listed in order of each of the Charter questions, as grouped by category (A-G). For each recommendation, the level of consensus attained within the WG has also been noted. Where, based on its analysis of the relevant public comments, the WG's final recommendation was changed substantially from its preliminary recommendation as reflected in the Initial Report, this has also been highlighted in the sections that follow.

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

WG Conclusion: ***Privacy and proxy services are to be treated the same way for the purpose of the accreditation process.***

The WG also agreed to adopt the definitions of privacy and proxy services that are in the 2013 RAA, as follows:

- ***"Privacy Service"*** means 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 privacy or proxy service provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services[51].

[51] The definitions of Privacy Service and Proxy Service reflect those in the 2013 RAA. In this context, the 2013 RAA also defines "Registered Name" as a domain name within the domain of a gTLD, about which a gTLD Registry

- ***"Proxy Service"*** is a service through which a Registered Name Holder licenses use of a Registered Name to the privacy or proxy customer in order to provide the privacy or proxy 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 customer's contact information.
- ***"Affiliate"***, when used in this Final Report in the context of the relationship between a privacy or proxy service provider and an ICANN-accredited registrar, means a privacy or proxy service provider that is Affiliated with such a registrar, in the sense that word is used in the 2013 RAA. Section 1.3 of the 2013 RAA defines an "Affiliate" as a person or entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, the person or entity specified.

In relation to the definitions of a Privacy Service and a Proxy Service, the WG makes the following additional recommendation:

- ***Registrars are not to knowingly[52] accept registrations from privacy or proxy service providers who are not accredited through the process developed by ICANN. For non-accredited entities registering names on behalf of third parties, the WG notes that the obligations for Registered Name Holders as outlined in section 3.7.7 of the 2013 RAA would apply***[53].

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?

Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance, and "Registered Name Holder" is defined as the holder of a Registered Name.

[52] In this context, "knowingly" refers to actual knowledge at the time that the registration is submitted to the registrar. As implementation guidance, this knowledge would normally be obtained through a report to the registrar from ICANN or a third party.

[53] Section 3.7.7.3 of the 2013 RAA reads as follows: "Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name."

WG Conclusion: ***To the extent feasible, domain name registrations involving P/P service providers should be clearly labelled as such in WHOIS[54].***

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 service providers 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, such as 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. The WG noted that the feasibility of this recommendation may be affected by the fact that it may not be the P/P service provider that is responsible for entering the relevant information into WHOIS.

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 Conclusion: ***The WG recommends[55] that P/P service customer data be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Program Specification of the 2013 RAA (as updated from time to time). Moreover, in the cases where a P/P service provider is Affiliated with a registrar and that Affiliated registrar has carried out validation and verification of the P/P customer data, re-verification by the P/P service provider of the same, identical, information should not be required.***

[54] The WG acknowledged that implementing this recommendation may require analysis of the possible implications of adding another field to WHOIS. For clarity, references to "WHOIS" in this Final Report are to the current globally accessible gTLD Registration Directory Service as well as any successors or replacements thereto.
[55] Some WG members nevertheless expressed the view that the minimum verification or validation standards for accredited P/P services should ideally exceed those applicable to non-proxy registrations.

WG Notes on B-2:

Similar to ICANN's Whois Data Reminder Policy, P/P service providers should be required to inform the P/P service customer annually of his/her requirement to provide accurate and up to date contact information to the P/P service provider. If the P/P service provider has any information suggesting that the P/P service customer information is incorrect (such as the provider receiving a bounced email notification or non-delivery notification message in connection with compliance with data reminder notices or otherwise) for any P/P service customer, the provider must verify or re-verify, as applicable, the email address(es). If, within fifteen (15) calendar days after receiving any such information, the P/P service provider does not receive an affirmative response from the P/P service customer providing the required verification, the P/P service provider 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 Conclusion: ***All rights, responsibilities and obligations for registrants as well as those of accredited P/P service providers would need to be clearly communicated in the P/P registration agreement, including a provider's obligations in managing those rights and responsibilities and any specific requirements applying to transfers and renewals of a domain name. In particular, all accredited P/P service providers 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. Further details as to minimum requirements for rights, responsibilities and obligations may need to be developed.***

The WG also recommends that it be mandatory for all accredited P/P service providers to Relay to their customers any notices required under the RAA or an ICANN Consensus Policy (see the main text under Category E in this Section 7 for additional recommendations regarding Relay).

In addition, the WG recommends the following as best practices for accredited P/P service providers:

- ***P/P service providers 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 Expired Registration Recovery Policy and transfers to another registrar.***
- ***P/P service providers 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.***
- ***P/P service providers should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved online location such as the provider's own website) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication.***

WG Notes on B-3:

In relation to transfers and renewals, the WG noted the common practice among providers of terminating P/P service protection as part of the transfer process as well as pending changes to the IRTP regarding the consequence of disabling a proxy service under the IRTP. As a result, the WG developed recommendations that emphasize the need to clearly disclose these consequences to customers (NOTE: a sub group was also formed to explore practical ways to facilitate transfers without the need for termination – see Section 5.3, above).

The WG did not explore in detail a possible recommendation that P/P service 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[56]:

"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[57]?

[56] 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.

[57] 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

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.

WG Conclusion: ***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 P/P 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[58].***

However, during the deliberations leading up to the Initial Report, some WG members expressed the view that domain names that are actively used for commercial transactions (e.g., the sale or exchange of goods or services) should not be able to use or continue using P/P services. Accordingly, Charter Question C-1 presented some distinctions that created a division within the WG which were reflected in the Initial Report, and for which public comments were 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 in its answer to the Threshold question for this Category C, 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

---

answer others. The WG also noted that references to the "use" of a domain for specific purposes may also implicate content questions.

[58] [58] The WG notes that the WHOIS RT had specifically acknowledged that P/P services can be and are used to address legitimate interests, both commercial and non-commercial.

not think it either necessary or practical to prohibit domain names being actively used for commercial activity from using P/P services.

As reflected in the two views that were presented for community feedback in the Initial Report, other 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. Moreover, 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 asserted that in jurisdictions where similar legal 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. This 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 at the time, suggest defining “commercial” within the context of specific activities, and uses “trading” as an example. However, the WG discussion focused on the broader term “commercial” and on whether certain types of commercial activity would 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 group that supported disallowing domains used for online financial transactions with a commercial purpose from using P/P services. Accordingly, a possible definition of “transactional” was developed during the WG’s initial deliberations, as follows: *“[D]omains used for*

online financial transactions for commercial purpose should be ineligible for privacy and proxy registrations.".

In consequence, in its Initial Report, the WG asked for community feedback regarding the question whether *"registrants of domain names associated with commercial activities and which are used for online financial transactions [should] be prohibited from using, or continuing to use, P/P services."* Responses to an additional two questions were contingent on support for a positive response to the first question, i.e., a viewpoint that such registrants should no longer be allowed to use P/P services. These two additional questions were: *"If you agree with this position [the prohibition], do you think it would be useful to adopt a definition of commercial or transactional to define those domains for which p/p service registration should be disallowed? If so, what should the definitions be?"*

A WG Sub-Team[59] analyzed the thousands of comments received that either directly responded to the first question posed, or that appeared to the Sub Team to be highly relevant to it (such as the many comments that endorsed statements that support *"the use of privacy services by all, for all legal purposes, regardless of whether the website is "commercial")."* Numerically, an overwhelming majority of these comments answered the question posed in the negative and supported no restrictions on the use of P/P services. Most comments were vehemently opposed to any distinction between the commercial and non-commercial and felt that any change would be seen as an erosion of privacy, a lack of protection for home based/small businesses and to inhibit freedom of speech. Many also felt there was sufficient law and regulation in place to deal with disclosure of names if required by the courts. On the other hand, those few commenters in favour of prohibiting the use of P/P services by those with commercial or financial activities based this opinion on the prevention and investigation of crime.

Considerable public feedback was received that expressed concern over the lack of robust and practical definitions of the terms "commercial activity" and "online financial transactions", with some commenters noting that it would likely be very difficult to develop such definitions. Several commenters, representing significant groups of stakeholders, noted that a yes-or-no response to the first question posed was difficult because the WG had not presented an agreed-upon definition of these

[59] The deliberations, draft documents and reports from this Sub Team can be reviewed at https://community.icann.org/x/0YZCAw.

terms. The WG therefore concludes that it is difficult to assume that the many commenters who answered (in effect) that registrations used to engage in "commercial activities" or to carry out "online financial transactions" should continue to be allowed to use P/P services would necessarily have answered the question the same way with regard to all conceivable definitions of these terms.

In view of the fact that the current situation is one where there are no restrictions on uses to which domain names registered using these services may be put, the WG does not believe that the accreditation standards for P/P services should require service providers to differentiate between registrants who wish to use these services to engage in commercial activities or online financial transactions and registrants who do not. This conclusion seeks to reflect the clear majority of opinions expressed in the comments, but also rests on pragmatic grounds, It will certainly be difficult (at best) to achieve a consensus definition of critical terms that must be defined in order to incorporate this principle into accreditation standards, and the WG does not support delaying the adoption and implementation of an accreditation system until such a consensus can be reached.

The WG notes that some P/P providers currently have enforce similar restrictions on who may use their particular services. The WG's conclusion that such a prohibition should not be incorporated into accreditation standards at this time is not meant to discourage accredited providers from adopting and implementing such policies if they so choose (provided that other relevant criteria, such as publication of terms of service and grounds for termination of the service, are fulfilled).

The WG also notes that at least some registrants engaged in commercial transactions using domain names registered through P/P services are doing so to carry out illegal activities or other abuses that may provide a basis for Disclosure or Publication under another part of these accreditation standard, or under terms of service adopted and published by accredited providers. For the avoidance of doubt, the WG's conclusion that registrants engaged in commercial or transactional activities should not be considered per se ineligible to use P/P services should have no impact on a particular registrant's eligibility (or not) to do so on other grounds.

Many commenters were also extremely concerned about the potential unintended consequences that could arise from barring the use of P/P services by certain types of registrants. There was an unqualified

wave of support for the principle that policy must not unduly restrict the use or P/P services at the expense of fundamental rights.

The following list summarizes what the WG believes, as a result of its review, to be some of the genuine and legitimate concerns expressed by many commenters:

- Doxing/SWAT-ing and concerns about physical safety (e.g. stalking, harassment or where registrant is in an unsafe or threatening location)
- Anonymity needs for certain individuals and organizations (e.g. those serving at-risk communities, targeted minorities, women and political and religious activists)
- Lack of separation of online business presence from personal information, in some cases for cost reasons and especially for home-based or small businesses (e.g. online shop owners, freelancers, self-employed persons, writers)
- Registrants who use pseudonyms and pen names for legal reasons (e.g. adult entertainers, erotica authors)
- Data harvesting concerns
- Spam, scams and identity theft (e.g. phishing attempts)
- Other legitimate need for privacy of domain information, e.g. new product launches, business competitors, pre-launch websites

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?

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

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 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.***

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

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

WG Notes on D-1:

The WG noted that provider responsiveness is a separate but necessary part of the accreditation program. While not necessarily fully dispositive of the issue of responsiveness for all the types of reports and requests that a P/P service provider may receive, the WG has developed a set of recommendations concerning the relaying of electronic communications, as well as an illustrative Framework to govern provider intake, processing and response to information disclosure requests from intellectual property rights-holders (see the main text in this Section 7 under Categories E and F below for details on the WG's recommendations concerning Relay and Disclosure procedures).

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 Conclusion: ***P/P service providers must maintain a point of contact for abuse reporting purposes. In this regard, 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. For clarification, the WG notes that as long as the requirement for a single point of contact can be fulfilled operationally, it is not mandating that a provider designate a specific individual to handle such reports. The WG also recommends that the designated point of contact be "capable and authorized" to investigate and handle abuse reports and information requests received.***

WG Notes on D-2:

The WG notes 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 of the RAA, and agrees that these recommendations may be helpful in developing guidelines and processes during the implementation phase of the WG proposals for this Charter question: (i) provide guidance to an abuse report requirement as to the types of abuse complaints allowed and types of actions P/P service 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).

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

WG Conclusion: ***The WG agreed that P/P service providers should be fully contactable through the publication of contact details on their websites in a manner modelled after Section 2.3 of the 2013 RAA Specification on Privacy and Proxy Registrations*** (as updated from time to time)***.***

WG Notes on D-3:

The WG notes that adoption and implementation of its recommendations in response to other Charter questions may have an effect on how this recommendation will be implemented (e.g. the WG recommendation for ICANN to publish a publicly-accessible list of accredited providers (see WG Conclusion for D-1), and for WHOIS entries to be clearly labelled if they are those of a P/P service provider (see WG Conclusion for B-1).)

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 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 P/P 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[60] or Safeguard 2, Annex 1 of the GAC's Beijing Communique[61] could serve as starting points for developing such a list.

The WG recommends that a uniform set of minimum mandatory criteria for the purpose of submitting abuse reports and information requests be developed. Forms that may be required by individual P/P service providers for this purpose should also include space for free form text[62]. P/P service providers should also have the ability to "categorize" reports received, in order to facilitate responsiveness.

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 Conclusions: The WG divided its discussions on Category E into two further topics, as further detailed below. The first set of recommendations concern provider obligations in terms of forwarding an initial electronic communication. The second set of recommendations concern provider obligations in relation to the escalation of relay requests by the requester of the initial communication.

I. Regarding Electronic Communications[63]:

(1) All communications required by the RAA and ICANN Consensus Policies must be Relayed.

---

[60] "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."

[61] "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."

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

[63] 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.

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

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

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

The WG also recommends that the use of standard forms and other mechanisms that would facilitate the prompt and accurate identification of a Relay request be explored during implementation (e.g. drop-down menus in a provider's web-based forms or fields that would require the filling in of a Requester'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

- ***All third party electronic requests alleging abuse by a P/P service customer will be promptly Relayed to the customer. A Requester will be promptly notified of a persistent failure of delivery[64] that a P/P service 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.***

[64] 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.

- ***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 upon request Relay a further form of notice to its customer. A provider should have the discretion to select the most appropriate means of Relaying such a request. A provider shall have the right to impose reasonable limits on the number of such requests made by the same Requester for the same domain name.***
- ***When a P/P service provider becomes aware of a persistent delivery failure to a customer as described herein, that 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 P/P service 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 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's final recommendations on the Category F Charter questions are set out below. The nature of its deliberations has meant that the WG believes it is more helpful to present its recommendations in a different form rather than as chronological answers to each Charter question.

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 more generally in all 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 Requester 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.***
- ***"Requester", when used in the context of Relay, Disclosure or Publication, including in the Illustrative Disclosure Framework described in Annex B, means an individual, organization or entity (or its authorized representatives) that requests from a privacy or proxy service provider either a Relay, or Disclosure or Publication of the identity or contact details of a customer, as the case may be.***

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 a similar 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. This definition is based on Section 3.18.2 of the 2013 Registrar Accreditation Agreement, which provision spells out a registrar's obligation to maintain a point of contact for, and to review reports received from, law enforcement authorities[65]; as such, the WG notes that its recommendation for a definition of "law enforcement authority" in the context of privacy and proxy service accreditation should also be updated to the extent that, and if and when, the corresponding definition in the RAA is modified.***

II. General Recommendations on Publication and Disclosure

The WG reviewed the Publication and Disclosure practices of several P/P service providers, some of who 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 practices were intended to encourage the Requester 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 P/P service providers to review requests manually or to facilitate direct resolution of an issue between a Requester and a customer. It also

[65] See https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

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 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 Requester. 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 P/P service providers should indicate clearly in their terms of service when they are referring to Publication requests (and their consequences) and when to Disclosure requests (and their consequences). The WG further recommends that accredited P/P service 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[66]. In making this recommendation, the WG noted the changes to be introduced to the IRTP in 2016, where following a Change of Registrant a registrar is required to impose a 60-day inter-registrar transfer lock. The WG also recommends that accredited P/P service providers should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved***

[66] 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.

online location such as the provider's own website) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication.

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

III. WG Recommendations Specific to LEA Requests

Although the WG has developed an illustrative Disclosure Framework for the intake, processing of, and response to, Disclosure requests made by a copyright or trademark owner (see Annex B), it has not done the same for LEA Requesters, or requests made by other types of third parties. This was due in part to what the WG believes are likely to be important differences with how these Requesters would handle certain issues such as those related to authorization and confidentiality, and what the WG perceived as a relative lack of expertise on the matter within the WG given that there were few WG participants with a LEA background. ***In the event that a Disclosure Framework is eventually developed for LEA requests, the WG recommends that the Framework expressly include requirements under which at a minimum: (a) the requester agrees to comply with all applicable data protection laws and to use any information disclosed to it solely for the purpose to determine whether further action on the issue is warranted, to contact the customer, or in a legal proceeding concerning the issue for which the request was made; and (b) exempts Disclosure where the customer has provided, or the P/P service provider has found, specific information, facts, and/or circumstances showing that Disclosure will endanger the safety of the customer.***

IV. WG Recommendations Specific to Requests made by Intellectual Property Rights-Holders

The WG recommends the adoption of an illustrative Disclosure Framework that would apply to Disclosure requests made to P/P providers by intellectual property (i.e. trademark and copyright) owners. The recommended Framework includes requirements concerning the nature and type of information to be provided by a Requester, non-exhaustive grounds for refusal of a request, and dispute resolution. ***Please refer to Annex B for the full text of this proposed Disclosure Framework.***

The WG further recommends that a review of the Illustrative Disclosure Framework in Annex B be conducted at the appropriate time after the launch of the program and periodically thereafter, to determine if the implemented recommendations meet the policy objectives for which they were developed. Such a review might be based on the non-exhaustive list of guiding principles developed by the GNSO's Data and Metrics for Policy Making (DMPM) WG, as adopted by the GNSO Council and ICANN Board. As noted by the DMPM WG, relevant metrics could include industry sources, community input via public comment or surveys or studies. In terms of surveys (whether or providers, customers or requesters), data should be anonymized and aggregated.

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

All accredited P/P service providers must publish their terms of service, including pricing (e.g. on their websites). Additionally, the WG recommends that accredited P/P service 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) may opt to cancel its domain registration prior to and in lieu of Publication. However, accredited P/P service providers that offer this option should nevertheless expressly prohibit cancellation of a domain name that is the subject of a UDRP proceeding.

VI. WG Recommendations on Requester Notification

The WG recommends that accredited P/P service providers should indicate clearly, on their websites and in all Publication or Disclosure-related materials, that a Requester 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.

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

The WG's review of various P/P service 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 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 P/P service providers to include on their websites, and in all Publication or Disclosure-related policies and documents, a link to a either a request form containing a set of specific, minimum, mandatory criteria, or an equivalent list of such criteria that the provider requires in order to comply with such requests (including with reference to the proposed Disclosure Framework for intellectual property-related requests). The WG also recommends that P/P service providers be required to state the applicable jurisdiction in which disputes (including any arising under the Illustrative Disclosure Framework in Annex B) should be resolved on any forms used for reporting and requesting purposes.***

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 service provider's accreditation, and the termination by a P/P service provider of its service to a customer (e.g. for breach of the provider's terms of service by a customer). The WG developed the following general principles, to govern the development of a de-accreditation process that would take into account the consequences of de-accreditation of a P/P service provider for a customer, with particular reference to the paramount need to ensure that reasonable safeguards exist to protect the privacy of a customer.

WG Conclusions:

Principle 1: A P/P service customer should be notified in advance of de-accreditation of a P/P service provider. The WG notes that the current practice for registrar de-accreditation involves the sending of several breach notices by ICANN Compliance prior to the final step of terminating a registrar's accreditation. While P/P service provider de-accreditation may not work identically to that for

registrars, the WG recommends that ICANN explore practicable ways in which customers may be notified during the breach notice process (or its equivalent) once ICANN issues a termination of accreditation notice but before the de-accreditation becomes effective. The WG recommends that de-accreditation become effective for existing customers thirty (30) days after notice of termination. The WG notes that, in view of the legitimate need to protect many customers' privacy, the mere publication of a breach notice on the ICANN website (as is now done for registrar de-accreditation) may not be sufficient to constitute notification.

Principle 2: Each step in the de-accreditation process should be designed so as to minimize the risk that a customer's personally identifiable information is made public.

Principle 3: The WG notes that the risk of inadvertent publication of a customer's details in the course of de-accreditation may be higher when the provider in question is not Affiliated with an ICANN-accredited registrar. As such, implementation design of the de-accreditation process should take into account the different scenarios that can arise when the provider being de-accredited is, or is not, Affiliated with an ICANN-accredited registrar.

In addition to the three principles outlined above, ***the WG recommends specifically that, where a Change of Registrant (as defined under the IRTP) takes place during the process of de-accreditation of a proxy service provider, a registrar should lift the mandatory 60-day lock at the express request of the beneficial user, provided the registrar has also been notified of the de-accreditation of the proxy service provider.***

The WG further recommends that the next review of the IRTP should include an analysis of the impact on P/P service customers, to ensure that adequate safeguards are in place as regards P/P service protection when domain names are transferred pursuant to an IRTP process. Where a P/P service customer initiates a transfer of a domain name, the WG recognizes that a registrar should have the same flexibility that it has currently to reject incoming transfers from any individual or entity, including those initiated by accredited P/P services. Nevertheless, ***the WG recommends that, in implementing those elements of the P/P service accreditation program that pertain to or that affect domain name transfers and in addition to its specific recommendations contained in this Final Report, ICANN should***

perform a general "compatibility check" of each proposed implementation mechanism with the then-current IRTP.

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 accredited P/P service providers are to publish certain minimum terms regarding Disclosure and Publication in their terms of service. The WG discussed but did not take a final position on whether these minimum recommendations are sufficient to ensure adequate protection of P/P service 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 for minimum mandatory requirements 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*
- *Whether a customer will have the option to cancel its domain name registration prior to and in lieu of Publication*

Other WG General Recommendations and Conclusions:

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 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.

In addition, the WG recommends that ICANN develop a public outreach and educational program for registrars, P/P service providers and customers (including potential customers) to inform them of the existence, launch and features of the P/P service accreditation program.

The WG further recommends that providers should be required to maintain statistics on the number of Publication and Disclosure requests received and the number honored, and provide these statistics in aggregate form to ICANN for periodic publication. The data should be aggregated so as not to create a market where nefarious users of the domain name system are able to use the information to find the P/P service that is least likely to make Disclosures.

8. Conclusions & Next Steps

The WG recommends that the GNSO Council adopt all the Full Consensus recommendations of the WG as presented in this Final Report, following the Council's review of the Report and the WG's processes.

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 – Illustrative Disclosure Framework applicable to Intellectual Property Rights-holder Disclosure Requests

By facilitating direct communication among Requesters, Providers, and Customers, this policy serves the public interest and seeks to balance the interests of concerned parties. It aims to give Requesters a higher degree of certainty and predictability as to if, when, and how they can obtain disclosure; to give Providers flexibility and discretion to act on requests for disclosure and not require that disclosure automatically follow any given request; and to include reasonable safeguards and procedures to protect the legitimate interests and legal rights of Customers of Providers. At an appropriate time after implementation of these accreditation standards and periodically thereafter, the Working Group recommends a review to determine whether these three objectives have been met and fairly balanced, as further described in Recommendation #19 of the Working Group's Final Report.

Policy Scope:

The following procedures were developed by the Working Group to apply to requests made by intellectual property rights-holders or their authorized representatives. The WG has not developed a similarly detailed process for other types of Requesters, e.g. law enforcement authorities or consumer protection agencies.

Given the balance that this Policy attempts to strike, evidence of the use of high-volume, automated electronic processes for sending Requests or responses to Requests (without human review) to the systems of Requesters, Providers, or Customers in performing any of the steps in the processes outlined in this Policy shall create a rebuttable presumption of non-compliance with this Policy.

I. Provider Process for Intake of Requests

- Provider will establish and publish a point of contact for submitting complaints that registration or use of a domain name for which the Provider provides privacy/proxy services infringes copyright or trademark rights of the Requester. The point of contact shall enable all the following information (in II below) to be submitted electronically, whether via email, through a web submission form, or similar means. Telephonic point of contact may also be provided.

- Nothing in this document prevents a Provider from implementing measures to optimize or manage access to the Request submission process. This could include:

  i. Requiring Requesters to register themselves and/or their organizations with Provider.

  ii. Authenticating complaint submissions as originating from a registered Requester (e.g., log- in, use of pre-identified e-mail address).

  iii. Assessing a nominal cost-recovery fee for processing complaint submissions, or to maintain Requester account so long as this does not serve as an unreasonable barrier to access to the process.

iv. Qualifying Requesters meeting certain reliable criteria as "trusted Requesters" whose requests would be subject to a streamlined process.

v. Revoking or blocking Requester access to the submission tool for egregious abuse of the tool or system, including submission of frivolous, vexatious, or harassing requests, or numerous Requests that are identical, i.e., that concern the same domain name, the same intellectual property, and the same Requester.

- Nothing in this document prevents Providers from sharing information with one another regarding Requesters who have been revoked or blocked from their systems or who have engaged in misconduct under this Policy, including frivolous or harassing requests.

- Nothing in this document prevents a Provider from adopting and implementing policies to publish the contact details of Customers in WHOIS, or to terminate privacy/proxy service to a Customer, for breach of Service Provider's published Terms of Service, or on other grounds stated in the published Terms of Service, even if the criteria outlined in this document for a Request have not been met.

II. Request templates for Disclosure

A. Where a domain name allegedly infringes a trademark

Requester provides to Provider verifiable evidence of wrongdoing, including:

1) The domain name that allegedly infringes the trademark;

2) Evidence of previous use of a relay function (compliant with the relevant section of accreditation standards regarding Relay) to attempt to contact the Customer regarding the subject matter of the request, if any, and of any responses thereto, if any;

3) Full name, physical address, email address, and telephone number of the trademark holder, and for legal entities, the country where incorporated or organized;

4) Authorized legal contact for trademark holder and his/her name, title, law firm, if outside counsel, physical address, email address and telephone number for contact purposes;

5) The trademark, the trademark registration number (if applicable), links to the national trademark register where the mark is registered (or a representative sample of such registers in the case of an internationally registered mark), showing that the registration is currently in force (if applicable), and the date of first use and/or of application and registration of the mark; and

6) A good faith statement, either under penalty of perjury or notarized or accompanied by sworn statement ("Versicherung an Eides statt"), from either the trademark holder or an authorized representative of the trademark holder, that:

a) Provides a basis for reasonably believing that the use of the trademark in the domain name

i. allegedly infringes the trademark holder's rights; and

ii. is not defensible.

b) States that Requester will comply with all applicable data protection laws while retaining Customer's contact details and will use Customer's contact details only:

i. to determine where further action is warranted to resolve the issue;

ii. to attempt to contact Customer regarding the issue; and/or

iii. in a legal proceeding concerning the issue; and

c) Agrees that the trademark holder will submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or trademark holder's knowing misuse of information disclosed to it in response to its request.

7) Where the signatory is not the rights holder, he/she must attest that he/she is an authorized representative of the rights holder, capable and qualified to evaluate and address the matters involved in this request, and having the authority to make the representations and claims on behalf of the rights holder in the request, including the authority to bind the rights holder to the limitations on the use of Customer data once disclosed.[67]

8) Where the signatory is not the rights holder, an officer of the rights holder (if a corporate entity) or an attorney of the rights holder, and the Provider has a reasonable basis to believe that the Requester is unauthorized to act on behalf of the rights holder or seeks to verify a new or unknown Requester, the Provider may request, and the Requester shall provide, sufficient proof of authorization.

B. Domain name resolves to website where copyright is allegedly infringed

Requester provides to Provider verifiable evidence of wrongdoing, including:

1) The exact URL where the allegedly infringing work or infringing activity is located, or a representative sample of where such work or activity is located;

[67] An example of such an attestation: "I attest that I am the rights holder / authorized representative of the rights holder, capable and qualified to evaluate and address the matters involved in this request, and have the authority to make the representations and claims in this request." The same attestation statement can also be used in situations arising under Section II.B(8) and Section II.C(7), below.

2) Evidence of previous use of a relay function (compliant with the relevant section of accreditation standards regarding Relay) to attempt to contact the Customer with regard to the subject matter of the request, if any, and of any responses thereto, if any. Requesters are also encouraged (but not required under this Policy) to provide evidence of previous attempts to contact the web host or the domain name registrar with regard to the subject matter of the request, if any, and of any responses thereto, if any;

3) Full name, physical address, email address, and telephone number of the copyright holder; and for legal entities, the country where incorporated or organized;

4) Authorized legal contact for the copyright holder and his/her name, law firm, if outside counsel, physical address, email address and telephone number for contact purposes;

5) Information reasonably sufficient to identify the copyrighted work, which may include, where applicable, the copyright registration number, and the country where the copyright is registered;

6) If possible, the exact URL where the original content is located (if online content) or where the claim can be verified; and

7) A good faith statement, either under penalty of perjury or notarized or accompanied by sworn statement ("Versicherung an Eides statt"), from either the copyright holder or an authorized representative of the copyright holder, that:

   a) Provides a basis for reasonably believing that the use of the copyright content on the website

      i. infringes the copyright holder's rights; and

      ii. is not defensible.

   b) Provides a basis for reasonably believing that the copyright protection extends to the locale the website targets

   c) States that Requester will comply with all applicable data protection laws while retaining Customer's contact details and will use Customer's contact details only:

      i. to determine whether further action is warranted to resolve the issue;

      ii. to attempt to contact Customer regarding the issue; and/or

      iii. in a legal proceeding concerning the issue; and

   d) Agrees that the copyright holder will submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its

home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or copyright holder's knowing misuse of information disclosed to it in response to its request.

8) Where the signatory is not the rights holder, he/she must attest that he/she is an authorized representative of the rights holder, capable and qualified to evaluate and address the matters involved in this request, and having the authority to make the representations and claims on behalf of the rights holder in the request, including the authority to bind the rights holder to the limitations on the use of Customer data once disclosed.

9) Where the signatory is not the rights holder, an officer of the rights holder (if a corporate entity) or an attorney of the rights holder, and the Provider has a reasonable basis to believe that the Requester is unauthorized to act on behalf of the rights holder or seeks to verify a new or unknown Requester, the Provider may request, and the Requester shall provide, sufficient proof of authorization.

C. Domain name resolves to website where trademark is allegedly infringed

Requester provides to Provider verifiable evidence of wrongdoing, including:

1) The exact URL where the allegedly infringing content is located;

2) Evidence of previous use of a relay function (compliant with the relevant section of accreditation standards regarding Relay) to attempt to contact the Customer with regard to the subject matter of the request, if any, and of any responses thereto, if any. Requesters are also encouraged (but not required under this Policy) to provide evidence of previous attempts to contact the web host or the domain name registrar with regard to the subject matter of the request, if any, and of any responses thereto, if any;

3) Full name, physical address, email address, and telephone number of the trademark holder; and for legal entities, the country where incorporated or organized;

4) Authorized legal contact for the trademark holder and his/her name, law firm, if outside counsel, physical address, email address and telephone number for contact purposes;

5) The trademark, the trademark registration number (if applicable), links to the national trademark register where the mark is registered (or a representative sample of such registers in the case of an internationally registered mark), showing that the registration is currently in force (if applicable), and the date of first use and/or of application and registration of the mark; and

6) A good faith statement, either under penalty of perjury or notarized or accompanied by sworn statement ("Versicherung an Eides statt"), from either the trademark holder or an authorized representative of the trademark holder, that:

a) Provides a reasonable basis for believing that the use of the trademark on the website

i. infringes the trademark holder's rights; and

ii. is not defensible.

b) States that Requester will comply with all applicable data protection laws while retaining Customer's contact details and will use Customer's contact details only:

i. to determine whether further action is warranted to resolve the issue;

ii. to attempt to contact Customer regarding the issue; and/or

iii. in a legal proceeding concerning the issue; and

c) Agrees that the trademark holder will submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or the trademark holder's knowing misuse of information disclosed to it in response to its request.

7) Where the signatory is not the rights holder, he/she must attest that he/she is an authorized representative of the rights holder, capable and qualified to evaluate and address the matters involved in this request, and having the authority to make the representations and claims on behalf of the rights holder in the request, including the authority to bind the rights holder to the limitations on the use of Customer data once disclosed.

8) Where the signatory is not the rights holder, an officer of the rights holder (if a corporate entity) or an attorney of the rights holder, and the Provider has a reasonable basis to believe that the Requester is unauthorized to act on behalf of the rights holder or seeks to verify a new or unknown Requester, the Provider may request, and the Requester shall provide, sufficient proof of authorization.

III. Provider Action on Request

Upon receipt of the verifiable evidence of wrongdoing set forth above in writing, Provider will take reasonable and prompt steps to investigate and respond appropriately to the request for disclosure, as follows:

A. Promptly notify the Customer about the complaint and disclosure request and request that the Customer respond to Provider within 15 calendar days. Provider shall advise the Customer that if the Customer believes there are legitimate reason(s) to object to disclosure, the Customer must disclose these reasons to the Provider and authorize the Provider to communicate such reason(s) to the Requester (so long as doing so will not endanger the safety of the Customer, as outlined in Section III(c)(vi)); and

B. Within 5 business days after receiving the Customer's response, or within 2 business days after the time for Customer's response has passed, Provider shall take one of the following actions:

   i. Disclose to Requester using secure communication channels the contact information it has for Customer that would ordinarily appear in the publicly accessible WHOIS for non-proxy/privacy registration; or

   ii. State to Requester in writing or by electronic communication its specific reasons for refusing to disclose.

   In exceptional circumstances, if Provider requires additional time to respond to the Requester, Provider shall inform the Requester of the cause of the delay, and state a new date by which it will provide its response under this Section.

C. Disclosure can be reasonably refused, for reasons consistent with the general policy stated herein, including without limitation any of the following:

   i. the Provider has already published Customer contact details in WHOIS as the result of termination of privacy/proxy service;

   ii. the Customer has objected to the disclosure and has provided a basis for reasonably believing (i) that it is not infringing the Requester's claimed intellectual property rights, and/or (ii) that its use of the claimed intellectual property is defensible;

   iii. the Provider has a basis for reasonably believing (i) that the Customer is not infringing the Requester's claimed intellectual property rights, and/or (ii) that the Customer's use of the claimed intellectual property is defensible;

   iv. the Customer has surrendered its domain name registration in lieu of disclosure, if the Provider offers its Customers this option;

   v. the Customer has provided, or the Provider has found, specific information, facts and/or circumstances showing that the Requester's trademark or copyright complaint is a pretext for obtaining the Customer's contact details by effecting removal of the privacy/proxy service for some other purpose unrelated to addressing the alleged infringement described in the Request;

   vi. the Customer has provided, or the Provider has found, specific information, facts, and/or circumstances showing that disclosure to the Requester will endanger the safety of the Customer; or

   vii. the Requester failed to provide to the Provider the verifiable evidence of wrongdoing outlined in Section II.

D. Disclosure cannot be refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to disclose be solely based on the fact that the Request is founded on alleged intellectual property infringement in content on a website associated with the domain name.

E. For all refusals made in accordance with the policy and requirements herein, Provider must accept and give due consideration to Requester's requests for reconsideration of the refusal to disclose.

F. A recommended mechanism for resolving disputes in which a Provider is alleged to have made a wrongful disclosure based on a Requester having provided false information is outlined in Annex 1 below.

Annex 1 To Disclosure Framework: Resolving Disputes Arising From Disclosures Made As A Result Of Allegedly Improper Requests

Notes:

For the avoidance of doubt, this option is not intended to preclude any party from seeking other available remedies at law.

Under these standards, disclosure is wrongful only when it is effected by the Requester having made knowingly false representations to the Provider. Disclosure is not wrongful if the Requester had a good faith basis for seeking disclosure at the time the Request was submitted to the Provider.

Under these standards, misuse occurs only when a Requester knowingly uses Customer contact information disclosed to it by a Service Provider for a purpose other than one of the specific purposes for which it had agreed to use such information (as listed in Section II.A(6), II.B(7), and II.C(6) of the Policy).

Jurisdiction:

In making a submission to request disclosure of a Customer's contact information, the Requester and the rights holder agrees to submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or rights holder's knowing misuse of information disclosed to it in response to its request.