PPSAI Implementation Analysis - Recommendation by Category, Difficulty of Implementing

How to Use This Document

This document provides a high-level analysis of the policy recommendations in the PPSAI Final Report. Please note that, although it was carefully drafted by ICANN staff, this document is a working document and may contain inconsistencies in language, brevity, or incomplete references. The Final Report was structured by answering charter questions labeled from A-F (with sub-numbering). In those answers, ICANN staff have reviewed and categorized the recommended policy requirements in the Final Report. The charts below show the estimated implementation difficulty or Level of Effort (LoE) for each category of the working group's (WG) answers to the charter questions. Each chart is labeled at a macro level with the highest LoE item determining its LoE assessment (e.g. if there are two categorized as "medium" and one as "high", the macro level label for that chart will be "high"). As mentioned above, these charter questions and their sub-numbering indicate the relevant Final Report Section(s) in the first column of each char). Each category of recommendations that collectively comprise the policy recommendations of the final report, include an accompanying rationale describing the difficulty/LoE rating. The rationale column also makes reference to existing draft policy and/or contract language stemming from the work completed with the previous Privacy & Proxy Services Accreditation Issues (PPSAI) Implementation Review Team (IRT). Each of the 17 charts below corresponds to a category of requirements as listed in the table of contents above. Finally, the rightmost column includes a comparison of the recommendations with existing requirements (e.g. in the Specification on Privacy & Proxy Registrations of the 2013 Registration Accreditation Agreement (RAA), the Temporary Specification, Transfer Policy, Registration Data Policy, etc.).

Recommendations are assessed according to an estimated difficulty / Level of Effort (LOE) rating

Low = No significant implementation challenges are expected for Implementation Planning Team(IPT)/IRT (two week task)

Medium = Additional IPT/IRT work will be required, because implementation of recommendations could be impacted by the Registration Data Policy, or Registration Data Request Service (RDRS), etc. (two month task)

High = Due to changed circumstances after the recommendations were adopted (in the marketplace, under ICANN Consensus Policy, and/or changes in law), it may not be practicable to implement these recommendations as originally contemplated in the PPSAI IRT. In some cases, the policy recommendations may need to be supplemented, changed, or GNSO Guidance may be required. (six month task). For these recommendations, before implementation efforts could re-start in the IPT/IRT, discussion may need to occur at the Board and/or GNSO level.

Accreditation - High

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
Other WG General Recommendations and Conclusions: 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 provider	High	The implementation approach taken in the PPSAI IRT was modeled on the registrar accreditation approach, whereby each Privacy/Proxy (P/P) provider would be required to apply for accreditation, be evaluated to ensure the provider met the accreditation criteria, etc. To this end, ICANN org had worked with the PPSAI IRT to develop a draft P/P Policy document, a draft Privacy and Proxy Service Provider Accreditation Agreement (PPAA), as well as related materials including a proposed accreditation process, fee structure, and other details. Given the changes in the marketplace, the fact that most or all P/P services known to ICANN are affiliated with registrars, and the changes in law, ICANN org believes that a more streamlined implementation approach would be beneficial. This could require discussion with the IRT and could require engagement at the	Yes, in the sense that registrars are accredited and accept registrations involving privacy and proxy services today, per requirements in the RAA. Implementation of the PPSAI recommendations will carry over some current requirements and adds some additional requirements.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
		Board/GNSO level.	
A2: Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process? Privacy and proxy services are to be treated the same way for the purpose of the accreditation process.	Low	There is a legal difference between privacy services and proxy services. This will impact the services' relationships with their customers and the registrar as well as the legal rights and obligations that the service provider has with respect to the domain name (proxy services are registrants, while privacy services are not). However, strictly from the perspective of the "accreditation process" there do not appear to be significant changes needed from the prior implementation-related efforts.	Yes, in the sense that the existing Specification to the RAA does not distinguish between privacy and proxy services (other than to define each type of service) so implementing new requirements that do not distinguish between these types of services for purposes of "accreditation" would not be a change from the current approach.
D3: 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 modeled after Section 2.3 of the 2013 RAA Specification on Privacy and Proxy Registrations (as updated from time to time).	Low	The draft PPAA would require publication of P/P provider contact information "on each website through which Provider provides or offers the Services" (see Section 3.11). In addition to this recommendation from the PPSAI (Policy Development Process (PDP), the Expedited Policy Development	Yes. The P/P Specification of the RAA requires, at Section 2.3 that "P/P Provider shall publish its business contact information on its website and/or Registrar's website." This recommended requirement would be a continuation of the current P/P Specification requirement.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
		Process) PDP on the Temporary Specification (Temp Spec) recommended that the full contact data of the P/P service must be published in RDDS. This PPSAI policy recommendation for the publication of P/P service contact data on the providers' websites could be implemented alongside the EPDP RegData Policy (so, once this policy is implemented, P/Ps would be required to publish their contact details on both their/the registrar's websites and in RDDS. *Noting however, that under the RegData Policy, it may not be clear that the contact information published in the RDDS belongs to a privacy or proxy service (for additional detail, see "Labeling" section below)).	
General mentions throughout the report 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	Low	These recommendations were accounted for in the PPSAI implementation efforts to-date. Section 3.11 of the draft PPAA would require privacy and proxy service providers to provide ICANN	No. However, Section 24 of the Registrar Information Specification of the RAA requires that the registrar provide ICANN with the following information: 1. Does the registrar or any of its

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
registrar (if any) as a requirement of the accreditation program.		with their business contact information and to keep this information up to date. Section 3.11.8 would require the P/P providers to disclose to ICANN the names and ICANN IDs of all affiliated P/P providers and affiliated registrars. The previous discussions with the PPSAI IRT envisioned that this information could be used to populate a publicly accessible list of these P/P providers and their contact information. No significant changes to this approach appear to be necessary.	affiliates offer any Privacy Service or Proxy Service (as such terms are defined in the Specification on Privacy and Proxy Registrations)? 2. If yes, list the entities or individuals providing the Privacy Service or Proxy Service.

Abuse Point of Contact - Medium

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
Category D2: 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? P/P service providers must maintain a point of contact for abuse reporting purposes. In this regard, the WG agreed that a	Low	Draft language to be included in a P/P accreditation agreement (PPAA) has been drafted, and can be repurposed to fit any revised implementation approach, such as inclusion of requirements in a policy document and/or Specification instead of a separate “accreditation	Similar requirement in P/P Spec to RAA, Section 2.2 (P/P required to publish abuse point of contact). The recommendation augments what currently exists by requiring that the contact be “capable and authorized” to investigate and handle abuse

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
"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.		agreement". See Section 3.12.1 of draft PPAA. This language (as with all the language originally discussed with the PPSAI IRT) will be reviewed again with the IRT, but no significant changes are expected. Potential data protection law (including GDPR) concerns can be mitigated by P/P providers publishing a role-based email instead of a name).	reports, which is greater than the minimal requirement to publish the contact and its reporting processes.
Category D4: 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? 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 or Safeguard 2, Annex 1 of the GAC's Beijing Communique 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	Medium	The draft PPAA, drafted in consultation with the PPSAI IRT, defines abuse as "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" (see draft PPAA at 1.1). Changes may be desirable to align with the approach taken in DNS Abuse amendments to the RA/RAA and any future work in the community with respect to	No. Current RAA requires that registrars must publish a point of contact for third parties wishing to report abuse or infringement of trademarks (or other rights). The Rr or the P/P must also publish the process or facilities for reporting abuse/infringement of rights (see P/P Specification to the RAA at 2.4.1). There are no obligations in the RAA P/P Specification to ensure they respond to reports, what abuse means or is covered.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
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. P/P service providers should also have the ability to "categorize" reports received, in order to facilitate responsiveness.		contracted party requirements for mitigating DNS Abuse.	

Communications - Medium

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
General mentions throughout the report **B3:** 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. **Other WG General Recommendations and Conclusions:** 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	Medium	The IRT should be consulted regarding whether any updates should be made to the prior language under consideration in the PPAA draft (see section 3.5.3.11). For example additional detail could be added or efforts made to align with implementation of the System for Standardized Access/Disclosure to non-public registration data (SSAD) recommendations concerning notices to data subjects if and when these recommendations are adopted by the Board. However, the policy recommendations are high-level and there is no legal reason why	No. This would be a new requirement for providers to communicate to their customers a clear explanation of what privacy and proxy services are (and how these services differ) as well as their corresponding obligations and responsibilities.

service accreditation program.		this policy recommendation could not be implemented as written.	

Definitions - Medium

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
A2: • **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. • **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.	Low	The definitions previously prepared in the draft documents developed with the PPSAI IRT, with the possible exception of "publication" (see below, Rationale for Category F in this section on Definitions, pp. 10-11) will not change as a result of the GDPR or EPDP.	Partially. The definitions of "Privacy Service" and "Proxy Service" are contained in the RAA Specification and are not significantly modified in the recommendation. In addition, the requirement to display the Privacy or Proxy Service contact information in the RDDS is required under the Temp Spec and Registration Data Policy, consistent with how they are defined in the recommendation. The RAA defines "Affiliate", as noted in the policy recommendation, and this would not alter that definition. Overall minor modifications are needed (i.e., remove privacy or proxy from the respective definitions where they conflict;

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
			update use of WHOIS due to WHOIS sunset).
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 accept registrations from privacy or proxy service providers who are not accredited through the process developed by ICANN. For nonaccredited 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.	Low	Draft P/P policy document developed in consultation with IRT contained language to effect this result.	Partially. RAA at Section 3.7.7.3 includes requirements concerning obligations for registered name holders who license use of domain names to a third party.
F: 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	Medium	ICANN should discuss with the IRT the concept of "reveal." The concept of "reveal" as described in the definition of "disclosure" is comparable to the concept of "disclosure" used in the Registration Data Policy, so it may be desirable to align terminology to avoid confusion across the policies. The concept of "reveal" as described in the definition of "publication" is also used throughout the Final Report, but may no longer be as relevant given the changes that have occurred with respect to registration data publication requirements under the new Registration Data Policy. The	Partially. While these definitions do not exist in the RAA or Registration Data Policy, the concepts of "disclosure" (comparable to the PPSAI's concept of "reveal") and "publication" were considered at length in the EPDP on the Temporary Specification for gTLD Registration Data and requirements related to disclosure were carried over in the Registration Data Policy.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
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, quasigovernmental 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; 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		team may wish to explore, in consultation with the IRT, whether terminology could be simplified to streamline the implementation of the policy without deviating from its intent. The concept of "publication" throughout the policy recommendations, and implementation of recommended requirements related to "publication," should be reviewed as a result of subsequent policies at ICANN. Now that much registration data is required to be redacted under prevailing privacy law(s) (rather than published in RDDS), this concept of "publication" is less relevant in today's marketplace than it was when the PPSAI recommendations were adopted. ICANN org, together with the IRT, may also need to consider the distinction between "publication" of registrant contact data in public RDDS versus the termination of the P/P service for the registration, which could result in the P/P customer data being redacted in RDDS, and the registrar being subject to consensus policy requirements for consideration	

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
corresponding definition in the RAA is modified.		of requests for disclosure of the contact information to a third party upon request instead of requirements concerning the reveal of customer contact data under the PPSAI recommended requirements (noting that registrar requirements regarding identity disclosure requests remain unchanged where privacy services are in place or terminated, and that registrar obligations under Registration Data Policy continue to be in effect). Notwithstanding this, including "publication" as a concept in PPSAI documentation isn't impossible or contrary to law.	

Differentiation - Low

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
C: The WG agrees that the status of a registrant as a commercial organization, noncommercial 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	Low	No apparent conflict between policy recommendation and data protection laws or subsequent policy developments at ICANN.	N/A - There are currently no requirements to distinguish between commercial and non-commercial organizations thus

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals			recommendations continue the status quo and do not conflict with data protection laws or other consensus policies.
C1: 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? - the WG agrees that the **mere fact of a domain being registered by a commercial entity, or by anyone conducting commercial activity in other spheres, should not prevent the use of P/P services**. In addition, a majority of WG members did not think it either necessary or practical to prohibit domain names being actively used for commercial activity from using P/P services. 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)	Low	No apparent conflict between policy recommendation and data protection laws or subsequent policy developments at ICANN.	N/A - There are currently no ICANN policy or contractual requirements to distinguish between domain names used for commercial versus personal purposes thus recommendations continue the status quo and do not conflict with data protection laws or other consensus policies.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
e) Must P/P services disclose affiliated interests? - 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."** - **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.** - 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 -			
C2: - **The WG does not believe that P/P registrations should be limited to private individuals who use their domains for**	Low	No apparent conflict between policy recommendation and data protection laws or subsequent policy	N/A - Currently no ICANN policy requirements exist to limit use of privacy and proxy services to private

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
non-commercial purposes.		developments at ICANN.	individuals, thus recommendations would continue the status quo.
C3: - **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.**	Low	No apparent conflict between policy recommendation and data protection laws or subsequent policy developments at ICANN.	N/A - Recommendations would continue the status quo.

Disclosure - High

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
F: - 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 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 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	Low	The draft PPAA developed in consultation with the PPSAI IRT broadly reflects these recommendations at Section 3.5.3; Section 3.5.1.12 would require the provider to specify in communications to the customer whether the provider is referring to "Publication" or "Disclosure", and explain the meaning and consequences of these actions (see 3.5.3.13).	Partially. RAA P/P Specification requires P/P providers to publish their terms of service, including the circumstances under which the P/P provider will reveal and/or publish the customer's identity or contact details (see RAA P/P Specification at 2.4.5). There is no prohibition in existing policies or contracts that would prevent P/P providers from manually reviewing requests or attempting to facilitate resolution of issues between requestors and P/P customers, so this would

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
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.			continue the status quo (provided that the details of the provider's practices must be disclosed in the required terms of service).
- 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. 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 interregistrar 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 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. -	Low	See, generally, requirements for P/P service Terms of Service at Section 3.5 of the draft PPAA; see, in particular, details concerning inter-registrar transfer lock at Section 3.5.3.11.2-3., Section 3.5.3.15 regarding link to the ICANN website where definitions of "publication" and "disclosure" can be found.	
- The WG further recommends that, in deciding whether or	Low	Draft language was included in draft	N/A- This is also not a

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
not to comply with a Disclosure or Publication request, providers not mandate that the Requester must have first made a Relay request.		PPAA at 3.17.2.	requirement of the Registration Data Policy with respect to requests for disclosure of nonpublic generic top-level domain (gTLD) registration data.
- 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	High	The EPDP on the Temporary Specification considered at length the requirements surrounding requests for disclosure of nonpublic contact data about domain name registrants. As a matter of ICANN policy, the community should consider whether the requirements for P/P services' consideration of comparable requests for data access should be aligned with the detailed requirements developed in EPDP Phase 1 and 2 (if and when Phase 2 recs are adopted by the Board). Alignment would be relatively easy from a drafting perspective, but the discussions on this topic could be extensive. However, because there is no recommended LEA framework as a matter of the PPSAI policy and the high-level requirements (a) and (b) could be implemented without creating a conflict with the Phase 2 EPDP SSAD Policy recommendations (if and when such recommendations are adopted by	No.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
		the Board), alignment would not require changes to the PPSAI policy recommendations.	
- 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	High	Framework should be reviewed in detail for any data protection law (including GDPR) issues. In addition, IRT should be consulted regarding the desirability of aligning this framework with the requirements of the Registration Data Policy and the EPDP Phase 2 recommendations (if and when these are adopted by the Board) to reduce a risk of confusion and to streamline processes for all parties involved.	No.
- 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.	Low	The Terms of Service (TOS) requirement doesn't appear to need changes.	Partially. See above (first item under Disclosure), in re existing RAA P/P Spec requirements and draft PPAA requirements concerning publication of P/P provider terms of service.
- The WG recommends that accredited P/P service providers should indicate clearly, on their websites and in all	Low	See draft PPAA, at Section 3.8 which includes these recommended	No, but see comparable requirements for contracted

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
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.		requirements. No significant implementation challenges, though the use of "publication" should be reviewed, as set out above.	parties' publication of terms concerning the mechanism and process for submitting disclosure requests at Registration Data Policy, at Section 10.
- 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.	Low	The recommended requirements for P/P services to link to a request form and criteria (and to include a forum-selection clause for disputes on all relevant forms) are not, themselves, difficult to implement. However, as noted elsewhere in this document, the implementation of specific criteria for requests is expected to require a "High" LoE. The community should consider whether alignment with the EPDP Phase 2 SSAD policy recommendations approach is desirable (if and when these recommendations are adopted by the Board).	No.
Other WG General Recommendations and Conclusions: 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	Medium	The draft PPAA, Specification 6, Reporting Specification, includes these recommended reporting requirements	No, as this creates a new requirement and reporting SLA to collect data and share with ICANN.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
use the information to find the P/P service that is least likely to make Disclosures.			

Labeling - Medium

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
B1: - **To the extent feasible, domain name registrations involving P/P service providers should be clearly labelled as such in WHOIS.** - the feasibility and effectiveness of these options should be further explored as part of the implementation process - 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.	Medium	Publication of the fact that a specific domain name registration is protected by a privacy or proxy service is not, itself, the processing of personal data (so does not raise significant data protection concerns that would require reconsideration of this recommendation). However, this recommendation will require additional effort to implement from a technical perspective. The prior proposed implementation of this recommendation should be revisited in consultation with the PPSAI IRT in light of changes to RDDS, the transition from WHOIS to RDAP, and to ensure that a technically workable and logical solution is implemented as a matter of ICANN policy concerning, specifically, the feasibility of whether and how such	No. The Registration Data Policy requires at 9.2.5 that the full registration data of the privacy or proxy service must be published in RDDS where a registration uses an affiliated or accredited privacy or proxy service. However, this is technically different from requiring a specific “label” on each registration involving P/P service providers. It may or may not be obvious, upon viewing the contact data for a P/P service in RDDS, that the registration is, in fact, a privacy or proxy protected registration. For example, for privacy service registrations, the registrant name and/or registrant organization would be redacted in public RDDS, so it could be difficult to determine upon viewing the RDDS record that

Final Report Section(s)	**Difficulty/LoE**	Rationale	**Does the requirement exist already?**
		labeling can and should occur. The technical complexity of creating an RDAP extension that signals that the registration is protected by either a privacy or proxy service and updating the RDAP profile to require the implementation of such an extension is categorized as Medium. However, the timeframe for full development of a new RDAP extension and an updated RDAP profile could be months or up to around two years.	this is a privacy registration. And, for proxy registrations, the name and contact information may or may not be clear on whether the registration is a proxy registration (this could depend on the viewer's familiarity with proxy service names and contact data).

Relay (Forwarding) of Third Party Requests - Low

Final Report Section(s)	**Difficulty/LoE**	**Rationale**	**Does the requirement exist already?**
B3: 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). - 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	Low	The proposed implementation of the recommendation concerning the relay of communications to P/P customers is not expected to need modification (see draft PPAA requirements concerning relay of notices required by RAA and Consensus Policies at Section 3.16).	No.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
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.		The Transfer Policy-related recommendations may require further consideration and could require coordination with current Transfer Policy review PDP. As noted above, a requirement for P/P providers to publish a link to an ICANN-approved resource of defined terms will not require a high LoE to implement, and this is already included in the draft PPAA language.	
E1: All communications required by the RAA and ICANN Consensus Policies must be Relayed. (2) For all other electronic communications, accredited P/P service providers may elect one of the following options: f Option #1: 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 f Option #2: 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.	Low	As noted above, implementation of a relay requirement is not expected to raise issues from a data protection perspective that would require a change from the prior approach taken to this requirement in the draft PPAA. Similarly, requiring P/P providers to publish information about a point of contact for requestors can be implemented as previously proposed.	No.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
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).			
E2: 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 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. 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.	Low	The initial draft requirement language does not appear to conflict with subsequent policy work.	No.

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
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/reverification (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.			

Reporting - Low

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
F: 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**.	Low	The recommended requirements for P/P services to link to a request form and criteria (and to include a forum-selection clause for disputes on all relevant forms) are not, themselves, difficult to implement. However, as noted elsewhere in this document, the implementation of specific criteria is expected to require a "High" LoE. The community should consider whether alignment with the EPDP Phase 2 SSAD policy recommendations is desirable (if and when these recommendations are adopted by the Board).	No.

		ICANN org should consult with the IRT to consider whether to align with DNS Abuse approach in RA/RAA and any subsequent community work in re DNS Abuse (perhaps to include a requirement that P/Ps implement any new abuse form requirements developed in the community or similar)	
General mentions throughout the report: 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. P/P service providers should also have the ability to "categorize" reports received, in order to facilitate responsiveness. 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. "Law enforcement authority" means law enforcement, consumer	Low	As noted above, for abuse reporting requirements, there would be benefits to alignment with the approach taken to defining and implementing requirements concerning DNS Abuse in the RA/RAA amendments. This would impact the types of reports to be received by the abuse contact, but would not directly impact the requirement for the P/P provider to have an abuse point of contact.	No.

protection, quasigovernmental 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; 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.			

Termination / Deaccreditation - Hard

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
G: 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 deaccreditation 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	Hard	This will need to be revisited in light of anticipated streamlined implementation approach.	No. The "de-accreditation" approach and process will need to be considered in light of the implementation approach agreed upon when the PPSAI is restarted. Additional consideration will need to be given to the relationship between the termination of a PP service versus termination of the registrar (or simultaneous termination of both types of services), and how the process should work. Implementation of a notification process for P/P customers will be feasible, but consideration will have to be given to how all of the relevant

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			requirements and processes fit together.

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.			

Terms of Service (TOS) - Low

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
B3: 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.	Low	Draft language was included in prior PPAA draft, and does not appear to require changes due to subsequent policy development or changes in law.	No.
F: 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. 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. 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 interregistrar transfer lock. The WG also recommends that	Low	As noted above, definitions may need to be revisited, but this particular requirement to include definitions in TOS would not be directly impacted.	No.

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 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. 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.			

Transfers - Low

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
B3: 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	Low	Requirement for communication of rights, responsibilities, and obligations for registrants and P/P service providers is estimated at a Low LoE to implement. At present, a standard inter-registrar transfer does not involve the removal of P/P services to effect the transfer.	No

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.		If a registrant is employing the services of a P/P service affiliated with a registrar and then opts to change registrars, the P/P services would generally not transfer to the new registrar, unless the two registrars were under the same parent company or were somehow affiliated. There could, for example, be a requirement that when a customer employing a Registrar's P/P services opts to transfer the name, there is a warning that the P/P services do not transfer with the name (if this is a concern).	
G: 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	Low	This is not a recommendation for PPSAI implementation, but for a separate Transfer policy review.	N/A

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.			

Verification & Validation - Low

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
B2: The WG recommends 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.	Low	See draft PPAA at Specification 1 (modeled on RAA RDDS Accuracy Program Specification).	Partially. Registrars must perform validation and verification requirements for the information collected under 3.3.1, which includes the underlying Registrant contact information with respect to a privacy service. In instances where the registration utilizes a Proxy Service, the Registrar must also perform verification and validation of the Account Holder contact information (which is the person/entity paying for or otherwise managing the registration). As such, in nearly all cases, the registrar of an affiliated P/P will have been required to perform the necessary validation/verification.

IP Disclosure Framework - High

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?

F : 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.	Medium	(See IP Disclosure Framework immediately below.) However, implementation of a requirement for a review at some future date does not seem challenging (because the work would occur *after* PPSAI implementation).	No.
Annex B contains the full Illustrative Disclosure Framework applicable to Intellectual Property Rights-holder Disclosure Requests	High	The proposed framework was reviewed with the PPSAI IRT and drafted for inclusion in the draft PPAA. However, subsequent developments, including the work of the EPDP on the Temporary Specification Phases 1 and 2, concerning similar subject-matter, should be discussed with the PPSAI IRT. It is possible the community could determine that it would be desirable to align the policy requirements and processes for disclosure for P/P contact data to those developed by the EPDP team for consistency and efficiency.	No.

Compatibility with existing policies - Medium

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
Work area not specified in Final Report. However, given the number of existing policies concerning areas that may overlap with the PPSAI recommendations, ICANN anticipates it will be necessary to review existing consensus policies to account for any impacts and updates to these.	Medium	As noted above, potential dependency with Transfer PDP. The Implementation Plan should include a review for any additional impacts on existing policies.	N/A

Data Processing Specification - Medium

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?
Work area not specified in Final Report. However, this is expected to be a relevant consideration for implementation of the PPSAI recommendations.	Medium	The Data Processing Specification (DPS) recommended in Phase 1 of the EPDP on the Temporary Specification is not yet implemented. It is expected that, once the DPS is finalized with respect to registrars' processing of personal registration data contemplated under the RegData Policy, this DPS could also be adapted to account for the processing of privacy and proxy customer data.	Not yet. The DPS is in the negotiation phase with contracted parties, and current thinking is that the DPS could be updated to account for the processing of privacy/proxy customer data.

Data Escrow Specification - Medium

Final Report Section(s)	Difficulty/LoE	Rationale	Does the requirement exist already?

Work area not specified in Final Report. However, this will be a necessary deliverable for implementation of the PPSAI recommendations.	Medium	Data escrow specification was drafted in consultation with PPSAI IRT. It should be revisited with PPSAI IRT in light of changes to data elements to be escrowed under RegData Policy.	No.

References

1. Draft 2018 IRT PPAA
2. Draft 2018 Policy Language on PPSAI
3. Draft 2018 Privacy and Proxy Service Provider Accreditation Program Applicant Guide
4. Draft 2018 Suspension, De-Accreditation and Transition Procedure
5. Draft 2018 Data Escrow Requirement Specification