

	A	B	C	D	E	F
1	Topic Area	Relevant Text From PDP Report	Specific Issue for Implementation	Specific Question for IRT	IRT Feedback	Proposed Resolution
2	Third-Party Requests	"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." (Final Report p.13)	How to implement this?	1. Is this approach to implementing this recommendation what the PDP WG intended?		1. Compile all known requirements for each type of request from Final Report. 2. IRT to identify gaps, considering: (a) who can submit a request; (b) what does request need to include; (c) required Provider actions in response to request; 3. Jointly develop solutions based on other known requirements (registrar) and industry best practices and known Provider practices
3	Abuse Reports	"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." (Final Report p. 12)	Known criteria (from Final Report): Who can report? Anyone;			
4	Abuse Reports	"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)." (Final Report p. 62)	How to Report? Unclear-- RAA requires abuse email but report seems to contemplate a form-based option	2. Can abuse reporting option be a form, or is email address required (mirroring RAA requirement?)		

	A	B	C	D	E	F
1	Topic Area	Relevant Text From PDP Report	Specific Issue for Implementation	Specific Question for IRT	IRT Feedback	Proposed Resolution
5	Abuse Reports	"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." (Final Report p. 12)	Report Criteria: Must allege abuse			
6	Abuse Reports	Lists of "abusive" activity referenced in Final Report are nearly identical (difference noted in red): Beijing Communique: 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. PICs Specification: 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.		3. Would adopting the list from the PICs Specification be consistent with PDP WG intent?		PICs specification and GAC Beijing Communique's lists of abusive activity are nearly identical. Adopting the list used in the PICs Specification would provide consistency across ICANN contracts.
7	Abuse Reports	"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." (Final Report p. 13)	Required Provider Actions for Receiving/Responding to Abuse Reports: Maintain designated point of contact who is capable and authorized to investigate and handle abuse reports and information requests received.	4. Where Final Report is silent on required Provider actions after receiving an abuse report, did WG intend for requirements to mirror RAA?		
8	Abuse Reports			5. If answer to question 4 is yes, would it be consistent with PDP WG intent to repurpose Section 3.18.1 of the RAA here to require that "Provider SHALL take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse."		

	A	B	C	D	E	F
1	Topic Area	Relevant Text From PDP Report	Specific Issue for Implementation	Specific Question for IRT	IRT Feedback	Proposed Resolution
9	Abuse Reports			6. If answer to question 5 is yes, did the WG intend any greater specificity here beyond the RAA requirement?		
10	Abuse Reports			7. If answer to question 4 is yes, would it be consistent with the PDP WG intent to repurpose Section 3.18.3 of the RAA to require that "Provider SHALL publish on its website a description of its procedures for the receipt, handling and tracking of abuse reports. The Provider SHALL document its receipt of and response to all such reports. The Provider shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, SHALL provide such records to ICANN upon reasonable notice."		
11	Relay Requests	"Regarding Relaying of Electronic Communications: All communications required by the RAA and ICANN Consensus Policies must be Relayed." (Final Report p. 13)	Who can request Relay? No restrictions on requests, but if Provider elects Option 2, then they are only required to relay communications from LEA and third parties that contain allegations of abuse			
12	Relay Requests	(Final Report p. 13): For all other electronic communications, P/P service providers may elect one of the following two options:	How can Relay be requested? Provider required to relay all electronic requests received, including those received via emails and web forms			

	A	B	C	D	E	F
1	Topic Area	Relevant Text From PDP Report	Specific Issue for Implementation	Specific Question for IRT	IRT Feedback	Proposed Resolution
13	Relay Requests	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	<p>Required Provider actions in response to Relay requests:</p> <p>1. Relay all communications required by the Registrar Accreditation Agreement and ICANN Consensus Policies; and either:</p> <p>2. Relay all electronic requests received (may implement safeguards to filter spam and abusive communications); or</p> <p>3. Relay all electronic requests received from LEA and third parties containing allegations of domain name abuse.</p>	8. For option 2, should "abuse" be defined consistently with the abuse reporting provision?		Defining these terms consistently would avoid any confusion that might arise from inconsistent definitions.
14	Relay Requests	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)		9. Do you see any gaps in required Provider actions on Relay where additional criteria may be needed?		
15	Relay Requests	(Final Report p. 14)"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.	Possible gap 1: Ensuring relayed communications reach Customer	10. Should Providers be required to test email forwarding to Customers to ensure forwarding is working properly?		

	A	B	C	D	E	F
1	Topic Area	Relevant Text From PDP Report	Specific Issue for Implementation	Specific Question for IRT	IRT Feedback	Proposed Resolution
16		"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 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)." (Final Report p. 14)				
17	Relay Requests	"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." (Final Report p. 14)	Possible gap 2: Timing of relay	11. Should there be a required timeframe for the mandatory Relay?		
18	Reveal	"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." (Final Report p. 10)	Who can request Reveal? No restrictions noted in Final Report			
19	Reveal	[Terms of Service SHALL include] 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 a registrar is required to impose a 60-day inter-registrar transfer lock." (Final Report p. 10)	How to request Reveal? No restrictions noted in Final Report; Report seemed to contemplate that a form (or other non-email option) could be used.			

	A	B	C	D	E	F
1	Topic Area	Relevant Text From PDP Report	Specific Issue for Implementation	Specific Question for IRT	IRT Feedback	Proposed Resolution
20	Reveal	[Terms of Service SHALL include] 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." (Final Report p. 10)	Required Provider Actions: ToS Requirements in Final Report only	12. Do you see any gaps where minimum mandatory criteria should be developed?		
21	Reveal	[Terms of Service SHALL include] 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." (Final Report p. 11)	Possible gap: Timing of response to Relay requests	13. Should there be target service level commitments for request responses?		