**Issues List Compilation – 28 January 2020**

| **#** | **Line number(s)** | **Cannot live with rationale** | **Proposed changes** |
| --- | --- | --- | --- |
|  | N/A | MUST have benefits of proposed SSAD:  It is important that the SSAD policy recommendations constitute an improvement over the status quo.  If in the estimation of this group, they are not an improvement, then we should not recommend them to the GNSO council.  In our proposed “next steps” document, the CPH team included in the appendix a list of advantages. We have further refined that list and request it’s inclusion in the draft.  The working group should agree on the expected improvements over the status quo. (RySG) | 1. Add to preamble or section 4.1 (principles)  **Single location to submit requests**    * Reduces time and effort spent by requesters to track down individual points of contact or follow individual procedures    * Ensures that requests are routed directly to the responsible party at each disclosing entity, thereby eliminating the uncertainty that requests are not received or go to someone unqualified to process them    * Allows for clear outreach opportunities to socialize the location and method for requesting non-public registration data    * Requests and responses can be tracked for SLA adherence 2. **Standardized request forms**    * Reduces the number of disclosure requests that are denied due to insufficient information    * Increases the efficiency with which disclosing entities can review requests    * Reduces uncertainty for requesters who now have a standard/uniform set of data to provide when submitting disclosure requests.    * Reduces the need for individual set of required information by disclosing parties 3. **Built-in authentication process**    * Speeds up the review process for disclosing entities as they will not need to re-verify the requestor    * External assurance that requestors have been verified can increase the likelihood and/or speed of disclosure 4. **Standardized review and response process**    * Allows creation of a common response format    * Allows creation of rules, guidelines and best practices disclosing parties can follow in reviewing and responding to requests    * Allows adoption of common response review system    * Allows automation of certain yet-to-be-defined requests by yet-to-be-defined requestors    * Facilitates automated disclosure decision making in some scenarios    * The logging of requests and responses also allows ICANN Compliance to audit the actions of disclosing entities, identifying any instances of systemic non-compliance, and take appropriate enforcement action |
|  | N/A | In the report where the discloser is identified, the report says contracted parties. While this has not specifically been discussed, we need to be clear that it is the registrar (who has the direct relationship with the data subject) who is responsible for the disclosure decision. (RySG) | Replace contracted parties with registrars (where applicable) throughout the report. |
|  | 39 | Didn’t we decide to harmonization instead of standardization? (ALAC) | Full automation4 of the SSAD may not be possible, but the EPDP 36 Team recommends that the SSAD must be automated where technically feasible AND legally permissible. Additionally, in areas where automation is not both technically feasible and legally permissible, **~~standardization~~** harmonization is the baseline objective. |
|  | 43 | Mechanism = not clear term needs elaboration/description/operating principles (GAC) | In recognition of the expected evolving nature of SSAD and in an effort to avoid having to conduct a PDP every time a change needs to be made, a **feedback** mechanism, which focuses solely on the implementation of the SSAD and does not contradict PDP and/or contractual requirements would need to be put in place to oversee and guide the continuous improvements of the SSAD. |
|  | 47 | (GAC) | ~~Meaningful~~ SLAs need to be put in place, but these may need to be of an evolutionary  nature to recognize that there will be a learning curve. |
|  | 51 | Not clear: from the relevant Contracted Party to the requestor (GAC) | Responses to disclosure requests, regardless of whether review is conducted manually or an automated responses is triggered, are returned from the relevant Contracted Party **directly** to the requestor, but appropriate logging mechanisms must be in place to allow for the SSAD to confirm that SLAs are met and responses are being processed according to the policy. |
|  | 66-67 | Not as discussed  Included recommendation to disclose (GAC)  *(Staff note: this diagram will be replaced by a detailed swim lanes that should provide further details. Diagram is expected to be reviewed on day 3).* | Central gateway reviews request for completeness and determines whether request meets criteria for automated response or Contracted Party Review. |
|  | 67 | We say CP but so far only a way to get to Rr. Need way to specify Ry. (ALAC) | In case of non-automated response, routed to CP for review and response to requestor. |
|  | 78-79 | Not as discussed  Needs to include the functions to collect data on decisions (GAC) | Central Gateway Manager – role performed by or overseen by ICANN Org. Responsible for managing intake and routing of SSAD requests that require manual review to responsible Contracted Parties. Responsible for managing and directing automated responses, consistent with the criteria established and agreed to in these policy recommendations. **Responsible for collecting data on disclosure decisions taken.** |
|  | 80 | “directing automated responses” unclear. “criteria agreed to in these policy recs” not really accurate (ALAC) | Central Gateway Manager – role performed by or overseen by ICANN Org. Responsible for managing intake and routing of SSAD requests that require manual review to responsible Contracted Parties. Responsible for managing and directing automated responses **by Contracted Parties**, consistent with the criteria established **by this process or the SSAD Advisory Group.**  ~~and agreed to in these policy recommendations~~. |
|  | 97 | SHOULD be automated (ALAC) | SSAD Advisory Group – Group consisting of ICANN community representatives responsible for advising ICANN Org and Contracted Parties on 1) SLA matrix review; 2) categories of disclosure requests which ~~should~~ **will** be automated; 3) other implementation improvements such as the identification of possible user categories and/or disclosure rationales. The Advisory Group may also make recommendations to the GNSO Council for any policy issues that may require further policy work. |
|  | 115-120 in conjunction with 220 - 224 | The failure to make the determination of who is the controller impacts the use of SHOULD or SHALL throughout the rest of the document with the respect of decision making (e.g. p. 17, line 704 - “the request may be denied”) (NCSG)  \*more of a comment, not the hill to die on  square bracket impacted language throughout the document, and provide a more detailed preamble.  *(note, proposed update is clean up to reflect single model is being recommended – no specific language has been provided yet by NCSG)* | ICANN Org provided its response on 19 November 2019 noting in part that “ICANN org proposed that it could operate a gateway for authorized data to pass through. As noted above, the gateway operator does not make the decision to authorize disclosure. In the proposed model, the authorization provider would decide whether or not the criteria for disclosure are met. If a request is authorized and authenticated, the gateway operator would request the data from the contracted party and disclose the relevant data set to the requestor”.  d) The decision to authorize disclosure of registration data, based on Validation of the Identity Credential, Authentication Credentials, and data as required in preliminary recommendation concerning criteria and content of requests, will reside with the registrar~~,~~ **and** ICANN~~, or whatever authorization provider the EPDP Team ultimately agrees on~~. |
|  | 161 | Not clear: what safeguards are for (GAC) | Accreditation - An administrative action by which the accreditation authority declares  that a user is approved to gain access to SSAD in a particular security configuration with  a prescribed set of safeguards **for performing legitimate requests**. |
|  | 170-171 | CLARIFICATION: This language seems to be confusing authentication with authorization. (ICANN Org) | Authentication - The process or action of Validating the Identity Credential ~~and Authorization Credentials~~ of a Requestor. |
|  | 180-184 | CLARIFICATION: As there is no third-party authorizer, are Authorization Credentials still relevant? (ICANN Org) | "Authorization Credential": A data object that is a portable representation of the association between an Identifier Credential and one or more access authorizations, and that can be presented for use in Validating those authorizations for an entity that attempts such access. Example: [OAuth  credential], X.509 attribute certificate. |
|  | 190-191 | CLARIFICATION: As above, is 2) still relevant given there are no third-party authorizers? (ICANN Org) | Identity Provider - Responsible for 1) Verifying the identity of a requestor and managing an Identifier Credential associated with the requestor and 2) Verifying and managing Authorization Credentials associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more 3rd parties. |
|  | 231 - 232 | CLARIFICATION: This seems to indicate an Identity Provider is required, but as the Accreditation Authority may also be the Identity Provider, this may benefit from a rewrite. (ICANN Org) | Management of Authorization Credentials: The Accreditation Authority MUST verify and manage a set of dynamic assertions/claims associated with and bound to the Identity Credential of the requestor. This verification, **which may be** performed by an Identity Provider, results in Authorization Credentials. |
|  | 296 | Provides transparency (GAC) | MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked**, complaints received** and information about the identity providers it is working with. |
|  | 311 | Clarity (GAC) | The revocation policy for individuals/entities should include graduated penalties. In other words, not every violation of the system will result in Revocation; however, Revocation may occur if the Accreditation Authority determines that the accredited individual or entity has materially breached the conditions of its accreditation and failed to cure based on: a) a third-party **verified** complaint received; b) results of an audit or investigation by the Accreditation Authority or auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. In the event there is a pattern or practice of abusive behavior within an entity, the credential for the entity could be suspended or revoked as part of a graduated sanction. |
|  | 383 | COMMENT: Consider only including definitions once, to avoid inconsistencies across recommendations or uncertainty during implementation. Not all definitions align with the definitions in Rec #1. (ICANN Org) | Preliminary Recommendation #2. Accreditation of governmental entities 1. Definitions |
|  | 450 - 452 | CLARIFICATION: Can the government in question make eligible any organization/ person in the world or can they only be limited to those in their jurisdiction? And is it any organization or person; or must it be a governmental entity? As an example, if a govt agency hires a third-party firm to assist with investigations, can they accredit that firm? (ICANN Org) | Accreditation by a countries’/territories’ government body or its authorized body would be available to various eligible entities that require access to non-public registration data for the exercise of their public policy task, including, but not limited to: |
|  | 613 | Urgent requests need immediate acknowledgement (GAC) | The EPDP Team recommends that the response time for acknowledging receipt of a SSAD request by the Central Gateway Manager must be without undue delay, but not more than two (2) hours from receipt. |
|  | 613 | Also need meantime targets rather than worst case targets (BC) | The EPDP Team recommends that the response time for acknowledging receipt of a SSAD request by the Central Gateway Manager must be without undue delay, but ~~not more than two (2) hours from receipt~~.**in a mean time of TBD seconds and not more than 2 hours.** |
|  | 615 - 619 | CLARIFICATION: Does the team intend for this confirmation to be a part of the Acknowledgement of Receipt? It reads in line 618 as it is part of the Gateway’s request response, not simply an acknowledgement. Can the team clarify? (ICANN Org) | The Central Gateway Manager MUST confirm that all required information as per preliminary recommendation #3, criteria and content of request, is provided. Should the Central Gateway Manager determine that the request is incomplete, the Central Gateway Manager must reply to the requestor with an incomplete request response, detailing which required data is missing,  and provide an opportunity for the requestor to amend its request. |
|  | 619 | This also needs a performance target (BC) | The Central Gateway Manager MUST confirm that all required information as per preliminary recommendation #3, criteria and content of request, is provided. Should the Central Gateway Manager determine that the request is incomplete, the Central Gateway Manager must reply to the requestor with an incomplete request response, detailing which required data is missing,  and provide an opportunity for the requestor to amend its request. **The reply must delivered in a mean time of TBD minutes but less than 2 hours”** |
|  | 627-630 | CLARIFICATION: Can the team clarify what is mean by “MUST review every request on its merits,” but also includes that “automated review is not explicitly prohibited where it is both legally and technically feasible.” (ICANN Org) | The Contracted Party to which the disclosure request has been routed MUST review every request on its merits and MUST NOT disclose data on the basis of accredited user category alone. For the avoidance of doubt, automated review is not explicitly prohibited where it is both legally and technically permissible. |
|  | 632 | Processors and joint controllers must not be disallowed (BC) | If deemed desirable, the Contracted Party may outsource the authorization responsibility to a third-party **processor\*** ~~provider~~, but the Contracted Party will remain ultimately responsible for ensuring that the applicable requirements are met.  **\*Note that joint controller scenarios may also be considered and this report makes no statement on the authorization responsibilities of the parties engaged in such agreements.** |
|  | 664-665 | Shouldn’t need permission to do this (IPC) | The Contracted Party may evaluate the underlying data requested once the validity of the request is determined under paragraph 4 above. |
|  | 670 | (BC)  Unclear language, and important policy principle (IPC) | The applicable lawful basis and whether the requested data contains personal data the authorization provider to determine if the balancing test, similar to the requirements under GDPR’s 6.1.f, as described in paragraph 6 below is applicable and proceed accordingly. **If there is no personal data in the request, the non-personal data MUST be disclosed.** |
|  | 680-82 | LE requests will likely be viewed as having potential to trigger legal proceedings; this language makes it sound like a negative factor; vague reference to ‘increased risk’, increased risk of what? (GAC) | Assessment of impact. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing (e.g., triggering legal proceedings). Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk for the data subject affected, this shall be taken into account during the decision-making. |
|  | 683 | Replace “processing” with “considering” (IPC) | Assessment of impact. Consider the direct impact on data subjects as well as any broader possible consequences of the data **considering** ~~processing~~ (e.g., triggering legal proceedings). Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk for the data subject affected, this shall be taken into account during the decision-making. |
|  | 701-705 | (BC) | **Where GDPR 6.1.f. is the cited legal basis**, if, based on consideration of the above factors, the Contracted Party determines that the requestor’s legitimate interest is not outweighed by the interests or fundamental rights and freedoms of the data subject, the data shall be disclosed. The rationale for the approval should be documented. |
|  | 727 - 760 | The Implementation Guidance language is not clear. When we discussed it, we couldn’t agree on what it meant or how it would be implemented. For example, we aren’t clear on who’s jurisdiction is applicable in the same jurisdiction requests  Need updated language to clarify the intent.  Also noted that automation is covered in Rec #7 and Rec #16, and should be consolidated. (RySG) | Implementation Guidance  The EPDP Team expects that the following types of disclosure requests can be fully automated (in-take as well as response) from the start:  • Law Enforcement in jurisdiction requests;  • Responses to UDRP Providers for registrant information verification. |
|  | 729 | CLARIFICATION: Does the SSAD Advisory Group determine which requests “can be responded to in an automatic fashion?” (ICANN Org) | For disclosure requests for which it has been determined that these can be responded to in an automatic fashion (i.e. no human intervention required) the following requirements will apply: |
|  | 741 | We should either put all the SLA type metrics in a single place, or else define them within the rec where they are applicable. I propose the latter. (BC) | ~~Responses to SSAD requests MUST be provided consistent with the SLAs outlined in preliminary recommendation #8.~~  Responses to SSAD requests must be provided with a meantime of TBD minutes and not more than 2 hours. |
|  | 744-7 | “sent to a CP” unclear (ALAC) | With respect to disclosure requests **that would have been sent to a Contracted Party for decision** ~~sent to a Contracted Party~~, a Contracted Party MAY request  the Central Gateway to fully automate all, or certain types of, disclosure requests, irrespective of the ultimate policy requirements. A Contracted Party MAY retract or revise a request for automation that is not required by these policy recommendations at any time. |
|  | 753 | Not clear (GAC)  CLARIFICATION: What does “in jurisdiction requests” mean? For example, is it the jurisdiction of the registry? Registrar? Where the servers are located? The headquarters of the relevant CP? Any location where the CP has employees or offices? How would this be automated? Would each CP have one or multiple jurisdictions? (ICANN Org) | Law Enforcement in **local** jurisdiction requests |
|  | 754 | Add examples from the examples given for automation (BC)  Needs to include more examples (IPC)  *(Staff note: leadership indicated that additional examples will be considered in parallel to the public comment phase)*  Add URS Providers (ALAC) | Responses to UDRP **and URS** Providers for registrant information verification. |
|  | 757 | “…can be fully automated” (ALAC) | The EPDP Team will further consider if other types of disclosure requests can be fully automated. Over time, based on experience gained and/or further legal guidance, the SSAD Advisory Group is expected to provide further guidance on which types of disclosure requests can be fully automated **Day 1**. |
|  | 761 - 808 | QUESTION: Some of these requirements include “should,” others “must.” Some are capitalized and others are not. Should these be harmonized? | Preliminary Recommendation #8. Response Requirements |
|  | 776-782 | MUST make a recommendation – will not always have suff. data to do that. (ALAC)  Replace SHOULD for MAY (BC)  Needs to be MUST (IPC)  CLARIFICATION: How would the Central Gateway Manager be expected to make a determination to disclose? On what criteria would it base this recommendation? Does the team expect that this would be an automated recommendation or would it require human review? Is this a functionality that is necessary for day 1? Or can it be built later as experience is gained? (ICANN Org) | As part of its relay to the responsible Contracted Party, the Central Gateway Manager ~~MUST~~ **MAY** provide a recommendation to the Contracted Party whether to disclose or not. The Contracted Party ~~MAY~~ **MUST** follow this recommendation. If the Contracted Party decides not to follow the recommendation of the Central Gateway Manager, the Contracted Party SHOULD communicate its reasons for not following the Central Gateway Manager recommendation so the Central Gateway Manager can learn and improve on future response recommendations. |
|  | 788 | “… must receive an automatic response with a meantime of TBD minutes and not more than 2 hours” (BC) | must provide a disclosure response without undue delay, unless there are exceptional circumstances. Such exceptional circumstances may include the overall number of requests received if the number far exceeds the established SLAs. SSAD requests that meet the automatic response criteria must receive an automatic disclosure response. For requests that do not meet the automatic response criteria, a response must be received ~~in line with the SLAs outlined below.~~ **with a meantime of TBD minutes and not more than 2 hours.** |
|  | 798 - 802 | Need recognition that Urgent Requests can be submitted by both LEA and non LEA. Submission by non-LEA should not require CP to consult with LEA first. Note that we have safeguards to hold non-LEA who abuse this process accountable, all the way to accreditation. (BC) | A separate accelerated timeline has been recommended for the response to ‘Urgent’ SSAD Requests, those Requests for which evidence is supplied to show an immediate need for disclosure (see below). The criteria to determine whether it concerns an urgent request are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation.  **The CP has the ability to determine whether a request meets the criteria. Note that the use of this capability is not limited to LEA, and the implementation should not put additional barriers to the use of this option by non-LEA requestors.** |
|  | 806 - 808 | Thought we agreed to display within SSAD portal to protect CPH (GAC)  *(Staff note – our understanding was that Central Gateway would have access to the dedicated contact information to relay requests, but this information would not be published)* | Must maintain a dedicated contact for dealing with Urgent SSAD requests which can be stored and used by the Central Gateway Manager, in circumstances where an SSAD request has been flagged as Urgent. Additionally, the EPDP Team recommends that Contracted Parties MUST publish their standard business hours and accompanying time zone on the homepage of their website (or in another standardized place that may be designated by ICANN from time to time). |
|  | 803-808 | This language does not reflect our recollection of what was discussed. Specifically, the second sentence is wrong. (RySG) | Must maintain a dedicated contact for dealing with Urgent SSAD requests which can be stored and used by the Central Gateway Manager, in circumstances where an SSAD request has been flagged as Urgent. ~~Additionally, the EPDP Team recommends that Contracted Parties MUST publish their standard business hours and accompanying time zone on the homepage of their website (or in another standardized place that may be designated by ICANN from time to time).~~ |
|  | 815-818 | First sentence:  We believe it was previously agreed to change the …complaint “should” be filed… to ….complaint “may” be filed  Second sentence:  We do not believe it’s possible or fair to ask ICANN compliance to “judge” a data controller’s decision to approve or reject a disclosure request (regardless of who the data controller is).  While we do feel that compliance can and should have a role in ensuring established policies and processes are followed, compliance is not in a position to compel disclosure when a data controller has determined that disclosure is not appropriate (RySG) | If a requestor is of the view that its request was denied erroneously, a complaint ~~should~~ **may** be filed with ICANN Compliance. ICANN Compliance must either compel disclosure or confirm that the denial was appropriate. ~~ICANN Compliance should be prepared to investigate complaints~~  ~~regarding disclosure requests under its standard enforcement processes.~~ |
|  | 834 | Not Clear (GAC) | An example of online critical infrastructure includes root servers; an example of offline critical infrastructure includes **utilities, transportation and banking etc.** |
|  | 836 - 887 | SLA not yet been discussed. (GAC)  We have issues with the SLAs and there hasn’t been the ability to discuss yet. We can’t support as drafted. We need an opportunity to discuss and agree to SLAs that we can live with. (RySG) | Preliminary Recommendation #9. Determining Variable SLAs for SSAD |
|  | SLA table 869 | Urgent requests are not subject to business schedules (BC) | Change “1 business day” 🡪 “1 calendar day” |
|  | SLA table 869 | Priority 3 SLA requires more discussion  Probably requires a small team to work through the latency (currently 5 days) and rate of compliance (currently 85%/90%/95%)  (BC) |  |
|  | 836 - 911 | Lines 848-849 says that initial priority will be set by the Central Gateway Manager based on criteria below, but there doesn’t seem to be information below. We don’t understand how priority is determined.  Lines 864-866 report isn’t clear on what happens when the registrar determines that a request identified as priority 1 isn’t priority 1. (RySG) | Who sets the priority?  The initial priority of a disclosure request is set by the Central Gateway Manager based on the criteria outlined below.  (…)  If a Contracted Party is of the view that the priority designation is not assigned by the Central Gateway Manager in a manner consistent with the conditions established by EPDP Team, the  Contracted Party can raise an appeal with the SSAD Steering Committee. |
|  | 842 | Market conditions unclear / Don’t know what this means (GAC) | Priority is a code assigned to requests for disclosure that contain agreed to, best effort target response times. The spectrum of codes is defined by urgency and corresponding impacts to match market conditions. It is assumed that the SSAD will contain an application to process disclosure requests and can manage a feature to set attributes for an inbound request in the SSAD. |
|  | 878 - 883 | there may be other laws that make it impermissible to disclose (NCSG) | These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention **if** **legally permissible**. |
|  | 933 | Needs to be specific. Include specific third-party purposes developed earlier (IPC) | Must, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, provide notice to data subjects of the types of entities/third parties which may process their data **such as (i) criminal law enforcement, national or public security, (ii) non law enforcement investigations and civil claims, including, intellectual property infringement and UDRP and URS claims, (iii) consumer protection, abuse prevention, digital service provider (DSP) and network security, or (iv) Registered name holder consent or contract.** |
|  | 1037 - 1042 | The policy needs to stipulate the retention requirements as per GDPR  (NCSG) | The EPDP Team recommends that requestors must confirm that they will store, protect and  dispose of the gTLD registration data in accordance with applicable law **and this policy will have to have a retention policy compliant with the GDPR.** |
|  | 1044 - 1106 | We would like to reiterate our position initial voiced at the first LA face to face that under no circumstances should data subjects (the registrants) be expected to pay for the ongoing maintenance of SSAD directly or indirectly. The ongoing maintenance and costs of running SSAD MUST be borne by the users (requesters) of the system. (RySG) | Preliminary Recommendation #15 Financial Sustainability  This needs to be clear in the Rec #15 language |
|  | 1066 | Replace “based on cost causation.” with “request volume or user type (e.g. governments may be legally prohibited from paying) among other potential factors.” (IPC) | The EPDP Team recognizes that the fees associated with using the SSAD may differ for users based on **request volume or user type (e.g. governments may be legally prohibited from paying) among other potential factors**. |
|  | 1068-1070 | Strike. Open to discussing (IPC) | ~~Under no circumstances should data subjects be expected to foot the bill for having their data disclosed to third parties; beneficiaries and users of the SSAD should bear the costs of maintaining this system~~ |
|  | 1110 | We thought there was agreement that automation should also be financially (or commercially) reasonable). (RySG) | The EPDP Team acknowledges that full automation of the SSAD may not be possible, but recommends that the SSAD must be automated where technically feasible**,** ~~and~~ legally permissible **and financially (or commercially) reasonable**. Additionally, in areas where automation is not both technically feasible and legally permissible, the EPDP Team recommends standardization as the baseline objective. |
|  | 1179 | Item addition (GAC) | Logging related to the accreditation provider  o Details of incoming requests for Accreditation  o Results of processing requests for Accreditation, e.g., issuance of the Identity  Credential or reasons for denial  o Details of Revocation Requests  o Indication when Identity Credentials and Authorization Credentials have been Validated.  **o Unique reference number** |
|  | 1229 - 1331 (and other references | The advisory group concept has not been flushed out to a degree that we are comfortable sending out to public comment as described in the draft. Further, it was our understanding and expectation that we would exhaust existing procedure and mechanisms before determining if creating a new process is needed. (RySG) | Remove Rec #19 and other references to SSAD advisory group.   We would be open to having as a question to the community IF existing mechanisms are sufficient or if a new mechanisms is needed. |
|  | 1296 | “advice” means something specific that I don’t think we mean here (e.g. GAC Advice), perhaps replace with “guidance”? | The Advisory Group will have the responsibility to provide ~~advice~~ **guidance** to ICANN Org and Contracted Parties on the following topics |
|  | 1283-90 | “If…” Thought that this was already decided. (ALAC) | [If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches of Registration Data held by ICANN in the SSAD. If such a breach is confirmed, Contracted Parties may withhold Registration Data from the SSAD until the Office of the Chief Technology Officer (OCTO) has confirmed that the breach has been remediated. In the event that such a breach has not been remediated, or is not expected by OCTO to be remediated within seven (7) days, a new SSAD provider should be brought online as quickly as possible but not longer than thirty (30) days from the date of identification of the breach.] |