GNSO Small Team's Review of the Operational Design Assessment

A. Please identify any clarifying questions you have in relation to the information provided in the ODA to assist with responding to the questions outlined below. These questions will be shared with the ICANN org ODP Team for their response.

#	Clarifying Question	ODA reference (page number, section)	From	Org's Answer
A1	Based on the general assumptions section on page 15, the ODA seems to be assuming an average of 4 requests per year per user via the SSAD. Is this correct and what was the basis for that assumption?	1.1 General Assumptions – page 15	Marc (RySG)	The ODA estimates: ● Between 25,000 and 3 million users ● Between 100,000 and 12 million requests submitted annually This means that the average number of requests per user per year could be anywhere from four (if it's either on low or high end for both volume and the user count) to 480 (if high end of volume with low end of user count). ICANN org examined several inputs to arrive at an estimated range. The data used included contracted party surveys (see Appendix 4 of the ODA), community surveys (see Appendix 5 of the ODA), a consideration of the rate of potential SSAD misuse, previous inputs from the EPDP Phase 2 Working Group and estimated numbers of law enforcement around the world. More information about data collection can be found in Appendix 3 of the ODA. It is important to note that our estimate was not based on market demand estimates. Rather, it was

				chosen so we could model systems and resources to support that range and scale.
A2	The table on page 59 has separate rows for “users” and “accreditation/identity Verifications”. What is the difference between the two and why are there more estimated accreditations/identity verifications for each volume estimate?	3.8 Fee Structure – page 59	Marc (RySG)	A user is someone who has had their identity verified and has a currently active account. A user may also be referred to as an Accredited Requestor. Each user will have, at minimum, one accreditation to validate their identity, but multiple forms/flavors/types of an accreditation can occur. This includes individuals, individual affiliation with a legal entity, and an individual’s representation of a legal entity. There are more accreditations estimated than users, because some users will require multiple accreditations.
A3	The accreditation fee seems to be based on a fixed $20 per accreditation cost. The variability in the numbers seems based solely on the volume of requests times that $20 dollar cost, plus enough margin to recoup the annual operating expenses and initial development costs over a 5-year period. Is that correct? Of the initial development costs, what amount is allocated to building the accreditation portion?	3.8 Fee Structure – pages 57 – 59	Marc (RySG)	The accreditation fee starts with a base assumption of $20 per accreditation, as this is our current estimate to outsource per transaction. Additionally, this includes recoupment for a portion of the annual operating expenses and a portion of the development and implementation costs. The recovery of the development and implementation costs was modeled to be recovered over a five-year period, ~$4M/yr. The annual recovery of the $4M is factored into the pricing for all three fees being charged and is dispersed relatively evenly amongst each fee: Accreditations verification, Requester declaration, and Disclosure requests.
A4	“Two systems must be built to deploy SSAD. ICANN org recommends outsourcing both. One is the Central AA system, [...] The second is the Central Gateway System, …” ● It could be one system with two main components/functions; should this option be considered (would it affect costs)?	Page 8	Sarah (RrSG)	System development costs have been estimated based on the functional components. Merging all components into a single system would have little to no impact on cost, because all functionality would still be required for integrating the Central Gateway with governmental accreditation authorities.

				The separation between the Central Gateway and central accreditation authority systems is due to the role of each system operator. The Central Gateway is expected to be an automated, centralized system to handle the receipt, management, and relay of disclosure requests between accreditation authorities (including governmental AAs) and contracted parties. The development of the Central Gateway is not expected to require specialized expertise from a software development perspective. On the other hand, the central accreditation authority system is expected to be outsourced to a separate entity, with specialized expertise around identity verification.
A5	The averages presented in the fee structure chart don't seem to be averages, can this be reviewed? E.g., Accreditation: low volume is $85.28, high volume is $21.30. 85.28+21.30=106.58. 106.58/2=53.29. Wouldn't the average for accreditation be $53.29 (not $22.22)?	Page 9	Sarah (RrSG)	The various scenarios are tied to the projected volumes. The volumes were initially projected in two scenarios - high and low. A third volume was developed (average) because there was a large range in the high and low volumes. All of the pricing and fees are tied to the low, average, and high volume. You cannot average the pricing; the volumes and costs need to be considered as they impact pricing.
A6	Central Gateway costs - Misuse management is double the work of base platform functionality, this seems odd? Can more info be provided about why?	Page 46	Sarah (RrSG)	The base platform estimate includes the initial standup and configuration of the base platforms that processes and functionality will be built atop. The Misuse management capabilities include enablement of operational workflows and customer facing features that span the monitoring, reporting,

				suspending, revoking, and reinstatement of misuse behavior within the SSAD. Our forecasts assumed that implementation of the Central Accreditation Authority base platform would likely yield reusable components and lessons learned (or vice versa, depending on sequencing). Therefore, the estimate for the base platform was reduced to reflect these efficiency gains.
A7	"While Implementation Guidance 1.8.2 indicates that Contracted Parties are provided with information about sanctioned Requestors, no need was identified for doing so, since Requestors that have breached the SSAD rules will be penalized as described in the form of suspension and/or revocation of their accreditation." ● Since requestors can go directly to the relevant Contracted Party to submit a disclosure request, it would be useful for the Contracted Party to know if that requestor has been found to be abusing the SSAD; this may reasonably factor into their disclosure decision (e.g. if the requestor was found to have falsified their identity).	Page 73	Sarah (RrSG)	Requestors going directly to contracted parties are outside of the SSAD, and as such, were not considered in the proposed design. The legal implications for processing requester personal data for this purpose should be considered in order to explore this option further. Additional functionality would also have an impact on development costs.
A8	Please explain the meaning of "users" (not defined under terminology) and how the numbers were developed (other than being in a 1:4 ration with disclosure requests). The numbers do not seem to agree with the number of accreditations. For instance, at the low volume, there are only 25,000 "users", but 60,00 entities have had their identity verified. At the high volume, the numbers are 4,000,000 verifications and just 3,000,000 users. Since accreditations need to be re-done every 2-5 years (Section 1.3), presumably after several years, the number of still valid cumulative	Page 59.	Alan (ALAC)	The number of accreditations would always be expected to outnumber users. Each user must be individually identified and certain users will need one or more accreditation processes to verify affiliation and/or representation. It is possible and expected that some users will need all three accreditation types. It is certainly possible that user and accreditation equilibrium (in which the system reaches a steady, predictable state) may not be reached for longer than the timeline provided within the ODA.

	accreditations will FAR outnumber the number of active users.			Please also see the response to A2.
A9	The number of requests per user seems rather low. Presumably this was a simple average with a distribution curve with some users making a large number of requests and others very few. Can ICANN Org please provide those distributions curves?	Page 59	Alan (ALAC)	ICANN org did not develop different distribution curves to develop the range. Please also see the response to A1.
A10	Amortization of the system development costs were included in the operational costs of the system. The SSAD Final report said that such costs MAY be included (section 14.7). Can you explain why the decision of whether or not to recover these costs, or have ICANN Org absorb them was not presented to the Board as an option? Moreover, the report (section 14.2) allowed ICANN Org to contribute to the operational costs further reducing the direct cost to users. Why was it decided that this option be ignored?	Pages 56-60	Alan (ALAC)	The fees that ICANN org is proposing assume full cost recovery, as outlined in the policy requirements in the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 EPDP. Full cost recovery includes design, implementation, and annual operating costs. ICANN org chose to include development costs as part of the full cost recovery to present the broadest possible impact of the policy recommendations. The design choices made for the purposes of the ODA are not meant to be proscriptive. Should the ICANN Board adopt the policy recommendations, it may direct the org to implement the recommendations differently than what is presented in the ODA.
A11	Regarding the Contracted Party responses to the survey, the report says: “Registrars reported they received a maximum of 699 requests a month. Registries reported they received a maximum of 1000 requests a month”	Page 110	Sarah (RrSG)	The language in this section of the ODA may have been confusing as the words “total” and “maximum” may be conflated. The analysis was done on an individual level, therefore the “maximum” amount corresponds to unique data requests reported to have been received from a single registrar or registry. It is important to note that the presented figures do not provide the full picture of data request queries

	● Does this mean when you combine all the responses from registrars the total is 699, or that one specific registrar reported 699? And same question for Registries. ● I think the intent is that it was the total for all Rr responders combined, but it is not clear in the document and I would ask that this be updated for clarity. Also, it is very difficult to compare CP responses to Community responses, because CPs are provided as a combined total while Community responses are not. If this can be adjusted so the results can be compared, that would be useful.			received and requested. Low participation rates and participants not completing the questionnaire in full made it more challenging to administer the survey. These challenges were also acknowledged and shared during our 24 September 2021 webinar, where we noted that our analysis presents a skewed and incomplete picture based on the reach of the survey and number of participants per organization type. To supplement the limited data received in the survey, ICANN org attempted to contract with a reputable market research firm to conduct a more thorough global analysis of potential market demand for the SSAD. ICANN org engaged with 11 firms and identified one that presented a suitable methodology for the work. However, the firm would not allow its name to be published with its reported findings, citing company and industry-wide practice. ICANN org confirmed with the GNSO Council small team that this lack of transparency would be of concern. Consequently, ICANN org has decided not to pursue work with the identified vendor at this time.
A12	"provided that the domain name is registered using a thick registry model." ● Instead of thick and thin, the report should focus on whether the registry holds registration data for that TLD	P. 81	Sarah (RrSG)	Thank you for the feedback. The team focused on thick registries, as the SSAD is intended for requesting redacted registration data.
A13	Figure 14. Estimated costs with base and high complexity & Figure 15. Estimated expenses at low, midpoint, and high volumes - Figures don't sum up. Please rectify or explain.	Page 56 & 57	Sebastien Ducos (Chair)	In addition to the displayed costs, there is a placeholder for contingency or unknown costs that we have less visibility into at the time of publication. The contingency is an amount included in the cost

				projections, but not specifically displayed in the Financial tables. It is critical to include a placeholder for unknown costs given the uncertainties that exist within the project. In Figure 14, the amount is $1,000,000 in the base complexity and $1,500,000 in the high complexity. In Figure 15, the amount is $160,000 in the low volume scenario, $200,000 in the average volume scenario and $230,000 in the high volume scenario.

B. Are there assumptions in the ODA that seem to be inconsistent or not aligned with the intent of the policy recommendations and/or EPDP Team deliberations?

#	Assumptions that seem to be inconsistent or not aligned with policy recommendations	ODA reference (page number, section)	From	Org's Answer
B1	The ODA seems to assume that the SLAs (recommendation 10) apply to the length of time the CP has to respond to a disclosure request letting the requestor know if their request has been approved or denied and that a separate timeline would exist for the CP to provide the data. That is not quite what the working group had in mind. The working group considered that SLA to be the amount of time the CP has to either respond with the data requested or provide a reason why the request has been denied.	2.2 Other issues – timely responses – page 21	Marc (RySG)	The proposed design considers the SLA and timeline for the Contracted Parties to either deny the access request with the corresponding rationale, or enable access for the requester directly to the registration data. The additional step to retrieve the registration data for approved data disclosure requests may be performed by the requester immediately after approval, but because this task is not performed by the contracted parties, it cannot be considered as part of the SSAD SLA defined in recommendation 10. The proposed process for accessing registration data prevents the disclosure of private registration data

				to other actors in the SSAD, aside from the requestor.
B2	The GAC shares this view with RySG as well; the SLA applies to the time to respond and either provide the data or deny the request with an explanation for the basis of the denial.	Same	Laureen (GAC)	Please see the response to B1.
B3	The ODA assumes that the various governmental and non-governmental accreditation authorities will also be the access point to the SSAD for requestors. That is not what the working group had in mind. The intent was for the Central Gateway to be the single point of entry for all SSAD users (thus the name). When accrediting a new user the Central gateway would leverage the applicable Accreditation Authority to verify the identity of SSAD users. The intake and processing of disclosure requests would be done directly to the Central Gateway (not via the accreditation authority as described in 3.3.1)	3.3.1 Disclosure request process – page 42 (and throughout the document)	Marc (RySG)	Interaction between requesters and accreditation authorities is required as part of the identity verification, as well as verification of relevant declarations applicable to disclosure requests. Pursuing the data minimization principle, it was proposed that only the accreditation authorities hold the requestor's personal information, which for the most part will not need to be processed by the Central Gateway. Requestors would also not need to deal with different entities when managing their accreditation, identity verification, billing, and submission of disclosure requests, as this would be handled through a single interface maintained by an accreditation authority. The org does not believe that this implementation approach contradicts the recommendation set within the Final Report. It should also be noted that the org's project team consulted with the GNSO Council on its understanding via the GNSO Council liaison, Janis Karklins, who shared the same view in his email to the Council dated 14 December 2021.

				There was no feedback received from the Council at that time.
B4	The GAC shares this view with RySG that all intake and processing of disclosure requests would flow through the Central Gateway. The GAC communicated to ICANN Org both orally, during meetings with staff, and in writing, about the inconsistency between what was set forth in the SSAD Recommendations and the view of the role of governmental accreditation authorities reflected in the ODA.	Same	Laureen (GAC)	Please see the response to B3.
B5	The diagram on page 77 shows a separate process for the requestor to go directly to the individual contracted party to get the non-public registration data (once approved). That isn't how the working group envisioned the SSAD working. Our expectation was that the central gateway would be the requestors single interface for requesting and receiving access to non-public registration data. This separate processes of going directly to the CP defeats some of the intended benefits and utility of having a single centralized system.	A1.10.8 RDAP Client – page 77	Marc (RySG)	This approach is in alignment with the high-level principles listed for the SSAD hybrid model in section 3.1 of Final Report of the Temporary Specification for gTLD Registration Data Phase 2 EPDP. The approach also is consistent with the responses to questions 15 and 16 received from the EPDP phase 2 working group in March 2020 (posted here),indicating that registration data does not go through the SSAD, but from the contracted party directly to the requestors. As described in the ODA, the proposal aims to leverage the advantages of the data access model proposed by the TSG, while ensuring that disclosed registration data does not go through other actors in SSAD other than the requestor.

B6	The GAC shares this view with RySG that the model proposed by the working group was to create a centralised system to increase ease of use and to allow for a more uniform system that would also reduce the impact on contracted parties.	Same	Laureen (GAC)	Please see the response to B5.
B7	"First, there is no standard duration or SLA from when the Contracted Parties approve a request to when they must allow Requestors access to the requested data" ● From §10.2 of the Final Report: "For purposes of calculating SLA response time, the EPDP Team recommends the SLA starts when a validated request with all supporting information is provided to the Contracted Party by the Central Gateway Manager and stops when the Contracted Party responds (via the Central Gateway) with either the information requested, a rejection response, or a request for additional information." ● Responding with the information requested (as in §10.2) seems to address this question of when they must allow requestors access to the data	Page 21	Sarah (RrSG)	Thank you for raising this point. The quoted text was a mistake on ICANN's part in the ODA. You may find the response to B1 to be of interest.
B8	"Once disclosure is approved, the original Requestor may query the data from the Contracted Parties' Registration Data Access Protocol (RDAP) service" "If disclosure is approved, the Requestor queries the approved registration data from the contracted party's RDAP service." ● Where did the assumption that it must be done through RDAP come from? And that the data is disclosed via the CP's RDAP service, external to the SSAD? How does the CP respond "via the Central	Page 8 Page 42 Pages 92-93, 95 (and elsewhere)	Sarah (RrSG)	Please see response to B5.

	Gateway" (Rec 10.2) but also through their own RDAP service? I think the expectation of the EPDP team was that responses go through the Central Gateway. Are CPs contractually obligated to perform work to make such a response via RDAP feasible?.			
B9	One of the vendor functions is "public relations services for an awareness campaign" ● Who is setting the budget for this campaign, and what will determine its success? ● Where is this represented in the Recommendations before the Board?	Page 8	Sarah (RrSG)	ICANN org will set the budget for this campaign by developing: ● Clear definition of external stakeholders ● Clear definition of the objectives, initiatives, and potential outcomes ● Timeline To determine success, the org and/or vendor will assess whether there is a marked shift in understanding and awareness among the target audiences. To do so, Specific measurements must be determined as the campaign is built. Success will be dependent on these factors: ● Close coordination with the Project lead ● Ample lead time to ramp up campaign (More than a couple of months if we are to hire an agency, etc.) While the policy recommendations do not explicitly include this effort, the org undertakes communications related to its work in many sectors. As the SSAD would be a new tool that may require educating interested users – including data subjects – the design contemplates a communications campaign to help reach those audiences. In addition, such a campaign may result in more informed use of the potential system.

B10	The report described “signed assertions” which could accompany accreditations. Examples included in the report were: • Assertion as to the legal basis of the request • Assertion that the user identified by the Identity Credential is affiliated with the relevant organization • Assertion regarding compliance with laws (e.g., storage, protection and retention/disposal of data) • Assertion regarding agreement to use the disclosed data for the legitimate and lawful purposes stated • Assertion regarding adherence to safeguards and/or terms of service and to be subject to revocation if they are found to be in violation • Assertions regarding prevention of abuse, auditing requirements, dispute resolution and complaints process, etc. The ODP (using the term Requestor Declarations) ignored all of those with the exception of verifying trademarks (or similar). The rationale given during an ODA presentation with the ALAC leadership team was that for the other types of assertion, they did not know how to “verify” them, which seemingly misses the point that most were not verifiable ahead of time but were in fact “promises”. Some, such as affiliation with a specific organization were likely verifiable. These assertions, although not mandatory that a CP use them, were in fact arguably among the most valuable aspects of accreditation as they could provide a CP with a level of comfort that the disclosed data would not be mis-used.	Page 17	Alan (ALAC)	The signed assertions described in the report were primarily related to future actions, but the concept related to signed assertions seemed related to delivering such verified assertions to Contracted Parties **prior** to the cContracted Party making a decision to disclose or not. If the concept behind the signed assertions related to future actions is that a user must be held to those promises as a matter of accreditation, then that area would be most appropriately verified after receipt of the data, perhaps significantly later, given the length of time that the data may be required for use due to policy-based usages such as UDRP or court actions or similar that may take years to finalize. ICANN was unable to determine a mechanism for these during the time-limited ODP, but in concert with the IRT process, it is certainly possible for such to be developed. Affiliation and representation verification were contemplated in the accreditation process and are mentioned in the responses to A2 and A9. Finally, the assertion related to verifying a power of attorney was considered, but will need the assistance of the IRT to understand the scope and nature of the verification sought.

B11	The ODA discusses the issue of controllership and data processing agreements. It includes the not-previously-heard statement that ICANN may be an independent controller in some cases and also states that the exact controller relationships cannot be determined until the "implementation details" are well understood. It is somewhat mind-boggling that the exact implementation of the SSAD would control the legal relationships. Surely the system should be designed and coded to meet the legal and relationship requirements and not the other way around. Moreover, if there are aspects where ICANN is the controller, that may alter the risk associated with CP which were central to many SSAD design issues. This needs further clarity.	Page 32	Alan (ALAC)	ICANN org has repeatedly stated that we believe that ICANN and the contracted parties each act as independent controllers with respect to the respective party's processing of registration data (see, for example, the 8 March 2018 "Cookbook" at p. 41, section 7.2.11.3, "ICANN has determined that each contracting party is acting as an independent controller in connection with the processing of WHOIS data.") As noted in a 14 January 2019 memo shared with the EPDP Team, "The possible status of ICANN org and the contracted parties as joint controllers or independent controllers is not a matter of the preferences of the parties, but it is ultimately a question of law about whether Article 26 of the GDPR applies." In that memo, ICANN org observed that the processing of gTLD registration data is not one set of "domain registration" operations. From ICANN org's perspective, gTLD registration data processing consists of various processing activities that occur under a common framework of agreements and policies. Under this framework, ICANN org and the contracted parties have separate and distinct purposes of processing, and each party exercises independent discretion on the means of such processing with respect to gTLD registration data. Therefore, the parties are independent and not joint controllers under the GDPR. ICANN org also asked the European Data Protection Board to please provide more clarity concerning how the principles of controllership would apply in a unified access model (see "Exploring a Unified Access Model for gTLD Registration Data"). In its 4 December 2019 response, the Belgian Data

				Protection Authority responded that even in a proposed Unified Access Model (where ICANN org would take on much more discretion concerning the data processing as compared to the recommended SSAD), the parties … are not free to simply ‘designate’ which party shall be deemed to act as a controller or joint controller. . . Instead, a factual and case-by-case assessment is necessary to determine the role of the parties involved.” The Belgian DPA did not provide any clarity concerning controllership in even a unified model, observing that “**Insofar as** ICANN acts as a joint controller, together with the registries and/or registrars, they must act within the boundaries of article 26 GDPR[.] (emphasis added)” ICANN org pointed out in the SSAD ODA that the identity of the controllers within an SSAD will depend on the specifics of how the SSAD is implemented (particularly, which entity or entities determine the purpose and the means of each processing operation within the SSAD). The SSAD ODA outlined one possible approach to implementing the SSAD, and additional details (the “who” will perform each aspect of the processing, and the mechanics of the processing (the “how)) will be determined in the implementation phase if and when ICANN org is directed to implement the SSAD by the Board. The “why” of the processing (the purpose), may also vary by party (for example, ICANN may have a purpose in furthering the security and stability of the DNS or ensuring registries’ and registrars’ compliance with contractual obligations, while the contracted parties or even contracted

				vendors and accreditation authorities may have different purposes for the processing). None of this is clear enough at this stage to determine, with any level of certainty, who the controller or controllers of such processing will be, and whether their controllership is independent or joint. Fundamentally, there has at times been a preoccupation with controllership labels, which misses the critical issue: Regardless of the label placed on the parties, the priority in implementing the SSAD, from a data protection perspective, is ensuring that data subjects' rights and freedoms under applicable law are met.
B12	As others have already commented, the concept of having data requests being made to the accreditation authority is neither what was specified in the report nor does it make sense in practice. For the typical case where ICANN (or its agent) is the AA and also operates the SSAD portal, it can be rationalized. But it makes no sense at all for the AAs that are separate from ICANN and specifically related to governments. Their accreditation action is a one-time event and they cannot be involved in a production operation. AA's must provide credentials that are then used in making operational requests to the SSAD. Since the SSAD must eventually need to accept the credentials of the government AAs, perhaps they need to be sub-AAs linked to the primary ICANN Org AA.	3.3.1 Disclosure request process – page 42 (and throughout the document)	Alan (ALAC)	Please see the response to B3.

C. Is there any information or issues that are not covered or not sufficiently covered that the ICANN Board would be expected to consider in its assessment of the policy recommendations?

#	Information / issues not covered or not sufficiently covered	ODA reference (page number, section)	From	Proposed Org's Answer
C1	Page 6: "In particular, the SSAD would facilitate the routing of requests for nonpublic gTLD registration data through a centralized system operated by ICANN org or its designee to the relevant contracted party. The contracted party, in its sole discretion, would determine whether to disclose the requested data" ● This high-level description of the SSAD omits the accreditation process		Sarah (RrSG)	As noted, this sentence is a brief, high-level description of the SSAD on page 6, which provides an Executive Summary. Please refer to Section 3.1.1 "Accreditation, Including Identity Verification" and Appendix 1 for the details of the accreditation process.
C2	Page 8: "For SSAD Requestors, AAs will be their only point of contact with the system. [...] AAs relay disclosure requests through the Central Gateway…" ● I had expected the CG would have a requestor interface; having all requestor interaction go through the AA is an interesting idea (better user experience) but does not match the Recommendations and should be further considered Page 29: "some GAC members raised concerns about the proposal to have all AAs serve as a "one-stop shop" for Requestors by both verifying identities and routing requests and payments for requests. [...] GAC members suggested that Governmental AAs' responsibilities be limited to verifying the identity of their users" ● If governmental requestors can't go through the AA to make requests and submit payment, how would they interact with the SSAD?		Sarah (RrSG)	For the user interface, please see the response to B3. For governmental requestors without access to a governmental accreditation authority, they would have to submit requests directly to the relevant contracted party. The Final Report contemplated that governments would only be able to gain accreditation via their own established accreditation authorities. The ODA on p. 29 notes: "Countries/territories may consider using a common vendor as an accreditation authority. A vendor may be able to offer such services to many governments. It is also possible that the vendor selected to provide the Central AA services may also be able to offer AA services to governments."

C3	Page 15: Carving out the risk mitigation, including cost for the legal risk fund, does not allow for an assessment of the overall operational cost. The ODA points to the question of “what role ICANN Org is slated to play in the final model”. Not only is the cost for the legal risk mitigation missing, but even the basis for such calculation, which goes back to the question whether ICANN considers itself as a processor or a controller (if so, what type of controller). With that information missing, it seems like no conclusive determination of the financial requirements seems to be possible.		Thomas (ISPCP)	As noted in footnote 3, should the Board direct ICANN org to implement the SSAD, further discussion will be required regarding a possible legal risk fund. The reason for not addressing the issue at this stage is that such an analysis would be complex and costly, involving considerable resources due to the unique nature of the SSAD and its global scope. For that reason, we believe it is sensible to have guidance from the Board before expending resources on this. While the EPDP Phase 2 recommendations specifically flagged the possibility of a legal risk fund, it’s possible that any fund created should address risk more broadly than legal risk. In addition, please see answer to question B11.
C4	Page 27: “The Central AA or a contracted IdP incorrectly verifies the identity of a Natural Person or incorrectly validates the existence of a Legal Person.” ● The real risk here is that the incorrectly verified person is able to make a disclosure request and receive data to which they have no legal entitlement.		Sarah (RrSG)	Thank you for your comments.

C5	Page 32 p: Whilst the report states that “an important first step for data protection compliance is identifying the controller(s) or the processing of personal data”, ICANN org does not seem to have taken this first step. During the work of the EPDP in Phase 1, ICANN Org was not willing to accept a determination of its role in the report. Now, the ODA states that “Controllers cannot be identified until the implementation details are solidified, because this will require assessing the facts of each data processing operation”. Where is the place, if not the ODA, where such assessment could be made? The ODA shall propose concrete implementation and should at least come up with a proposed allocation of responsibilities. This information is missing. If ICANN Org is not in a position to make a final determination, it should at least propose a workable model. Absent such proposal, it looks like we are moving in circles and cannot make progress.		Thomas (ISPCP)	ICANN org pointed out in the SSAD ODA that the identity of the controllers within an SSAD will depend on the specifics of how the SSAD is implemented (particularly, which entity or entities determine the purpose and the means of each processing operation within the SSAD). This will occur in the implementation phase, which will begin if and when ICANN org is directed to implement the SSAD by the ICANN Board. The SSAD ODA outlined one possible high-level approach to implementing the SSAD. The ICANN org and Board are receiving a variety of feedback on the proposed approach, via the community discussions and, in particular, the GNSO Council’s SSAD ODA Small Team. Additional details solidified during the implementation process, in consultation with the Implementation Review Team, including the party or parties who will perform each aspect of the processing, and the mechanics of the processing (the “when/where/how”) will be determined in the implementation phase if and when ICANN org is directed to implement the SSAD by the Board. For example, will a single vendor operate the gateway and also act as an accreditation authority? Will the accreditation authority serve as the entry point for submitting a request for access to data, as proposed in the SSAD ODA? These issues are not yet resolved, and could have an impact on controllership. The “why” of the processing (the purpose), may also vary by party (for example, ICANN may have a purpose in furthering the security and stability of the

				DNS or ensuring registries’ and registrars’ compliance with contractual obligations, while the contracted parties or even contracted vendors and accreditation authorities may have different purposes for the processing). None of this is clear enough at this stage to determine, with any level of certainty, who the controller or controllers of such processing will be, and whether their controllership is independent or joint. Fundamentally, there has at times been a preoccupation with controllership labels, which misses the critical issue: Regardless of the label placed on the parties, the priority in implementing the SSAD, from a data protection perspective, is ensuring that data subjects’ rights and freedoms under applicable law are met. Question B11 provides additional background concerning ICANN org statements to date regarding the issue of controllership with respect to the processing of personal data contained within registration data.
C6	Page 75: “the actual value of having the recommendations made available depends entirely on the Contracted Parties’ intent to incorporate them in their review process” ● Also depends on the recommendation itself; if the recommendations are bad, they won't be followed		Sarah (RrSG)	Thank you for your comments.

C7	Overall, the presentation of costs was far from clear. The actual net operational costs of the system (that is, the costs not recovered directly from users) was just $4.8M per year for the low volume scenario and $7.3M for the high volume scenario. This is VERY different from the high-level presentations only presenting the overall costs ($14M-$107M), the bulk of which would be paid by users who presumably believe they are getting value for money.		Alan (ALAC)	There are three primary categories of costs: Direct Expenses - These expenses vary significantly by scenario, as they are directly related to the amount of volume. Annual Operating Expenses - These expenses vary by scenario, but are fairly steady and not impacted by the range of volumes we have projected. Development and Implementation Costs to Recover - These costs are the same in all scenarios and are not impacted by volume. ICANN org chose to display the costs in these three categories so it was transparent which costs were driving the changes in each of our scenarios. This level of detail helps isolate which costs are fixed/stable and which are more fluid due to the volume.
C8	ODA Section 3.9.1.4 on risks associated with changes in laws needs further clarity. Clearly if some laws change that forbid doing something that ICANN policy requires, that is a problem that must be addressed. And if the SSAD implementation is counter to these laws, that to must be addressed. But the paragraph implies. But the paragraph also talks about standards for the disclosure. If for instance, new laws require disclosure within a specific time (less than implied by the SSAD SLAs), is the SSAD expected to adhere to these new standards? That is akin to ICANN enforcing laws, which is not likely in ICANN's mandate.		Alan (ALAC)	There are a variety of ways in which new laws could impact the SSAD. For example, if a new law (such as NIS2 in Europe) required the publication of additional registration data, SSAD usage would be expected to decrease, which could drive up the costs for the requests that continue to come in via the SSAD. If new laws restrict a contracted party's ability to disclose data to third parties, SSAD usage would also be expected to decrease. This also could impact a contracted party's ability to comply with recommended use cases to be automated (resulting in a contracted party opting out of such automated

				disclosures and manually evaluating such requests, resulting in a longer processing time). ICANN and the contracted parties must comply with all applicable laws. As a matter of ICANN policy, if new laws required specific processing times for a contracted party's request for access to nonpublic gTLD registration data, then this could be a topic for further policy development, or a need for a contracted party to encourage requestors to submit requests directly to the contracted party if any timelines or other measures required by law cannot be met via the SSAD.
C9	The note on page 65 regarding the word "standardized" is important. The system is far from providing a standardized service, and the use of the word should likely be omitted from the name going forward as keeping would unreasonably set expectations.		Alan (ALAC)	Thank you for your comment.
C10	It is not clear whether the impact of restrictions on the transfer of domain name registration data across borders has been factored into the estimates on usage. (this is noted as a Risk on p. 33).		Laureen (GAC)	ICANN org estimated the potential numbers of requestors and requests based on several factors outlined in Footnote 2 of the ODA: "ICANN org examined several inputs to arrive at an estimated range. The data used included contracted party surveys (see Appendix 4), community surveys (see Appendix 5), a consideration of the rate of potential SSAD misuse, previous inputs from the EPDP Phase 2 Working Group, and estimated numbers of law enforcement around the world. More information about data collection can be found in Appendix 3." Because the impact of cross-border transfer restrictions is not yet fully understood this was not

				factored into the ODA’s estimated ranges and noted it as a potential risk. Please also see the response to A1.
C11	The reference to the “disclosure decision recommendation engine” is not clear. P. 42. What would inform the Recommendation Engine? Who sets the criteria? Based on what parameters?		Laureen (GAC)	The recommendation engine was not contemplated in the proposed design. Please refer to Sections 3.3 and A1.8 of the ODA.