**Proposal for an SSAD Hybrid able to evolve to a Centralized and Automated Model (“The Chameleon”)**

21 January 2020

The following proposal aims to bring together the CPH Hybrid SSAD Model, the Centralized option for CPH Hybrid Model developed by Mark Svancarek and the subsequent input provided through the small team meetings and mailing list input. From the reactions of the different groups it appears clear that the hybrid model enjoys support from various groups but only if:

1. A commitment is made and confirmed in the policy recommendations that if/when confirmed legally permissible and not increasing liability for contracted parties, automatic responses to disclosure requests are to be implemented, without needing a new PDP;
2. Meaningful SLAs are agreed that result in timely responses to disclosure requests[[1]](#footnote-1).

The following principles underpin the high-level description of the SSAD Hybrid able to evolve to a centralized and automated model hereunder as well as the proposed modifications to the preliminary recommendations which can be found further below[[2]](#footnote-2):

* At this point in time, no legal opinion, guidance, or advice has been received that suggests that the type of liability shifting required under the centralized model is legally possible. However, such guidance or advice may be received at a later point in time, but waiting for this to happen could significantly delay the implementation of an SSAD.
* Full automation of the SSAD may not be possible, but 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 is the baseline objective.
* Experience gained over time with SSAD disclosure requests and responses must inform further streamlining and standardization of responses.
* No reliable data is available to assess the expected number of requests nor the breakdown of urgent vs ‘normal’ requests. This may make it difficult to determine or commit to response time requirements. It should also be recognized that the number of requests may fluctuate over time. Also, as a result of experience gained efficiencies are expected to develop.
* To deal with the expected evolving nature of SSAD from a hybrid to a (partly) centralized model and avoid having to conduct a PDP every time a change needs to be made, a standing committee of sorts would need to be put in place to oversee and guide the continuous improvements of the SSAD.

**High level overview of SSAD Hybrid able to evolve to a centralized and automated model**

1. Requestor obtains accreditation
2. Accredited requestor submits disclosure request to SSAD central gateway
3. Central gateway reviews request for completeness and determines whether request meets criteria for automated response or Contracted Party Review.

1. In case of non-automated response, routed

to CP for review and response to requestor.

1. In case of automated response, automated response

directly returned to requestor at direction of SSAD Central Gateway.

If deemed technically possible and legally permissible, the requests that are assessed to be eligible for an automated response are expected to grow over time, although it is not expected that all requests ultimately will end up in this category as it is the expectation that there are always edge cases that will require manual review.

**Main SSAD Roles & Responsibilities** (to be further detailed following agreement on proposal and preliminary recommendations):

* **Central Gateway Manager** – role performed by or overseen by ICANN Org. Responsible for managing intake and routing of SSAD requests to responsible Contracted Parties. Responsible for managing automated responses, following criteria established and agreed to by SSAD Steering Committee.
* **Accreditation Authority** – role performed by or overseen by ICANN Org. A management entity who has been designated to have the formal authority to "accredit" users of SSAD, i.e., to confirm and Verify the identity of the user (represented by an Identifier Credential) and assertions (or claims) associated with the Identity Credential (represented by Authorization Credentials).
* **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.
* **Contracted Parties** – Responsible for responding to disclosure requests that do not meet the criteria for an automated response.
* **SSAD Steering Committee** – Committee consisting of ICANN community representatives responsible for 1) reviewing and revising, as appropriate, the SLA matrix; 2) reviewing, confirming and establishing the criteria for which categories of disclosure requests must be automated (for example, local LE requests from a CP in jurisdiction); 3) reviewing and confirming other implementation improvements such as the identification of possible user categories and/or disclosure rationales.; 4) Make recommendations to the GNSO Council for any policy issues that may require further policy work.

It is the expectation that the different roles and responsibilities will be outlined in detail and confirmed in the applicable agreements.

**Updated preliminary recommendations from draft Initial Report**

*(note that updates only relate to changes that would bring the preliminary recommendations in line with the proposal described above – other comments and/or highlights have been removed for ease of reading.)*

1. **Accreditation[[3]](#footnote-3)**

Proposed working definitions used by the EPDP Team in its discussion of accreditation:

* **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.
* **Accreditation Authority** - A management entity who has been designated to have the formal authority to "accredit" users of SSAD, i.e., to confirm and Verify the identity of the user (represented by an Identifier Credential) and assertions (or claims) associated with the Identity Credential (represented by Authorization Credentials).
* **Accreditation Authority Auditor** - Independent entity that is contracted by ICANN org to carry out auditing requirements as outlined in auditing preliminary recommendation.
* **Authentication** - The process or action of Validating the Identity Credential and Authorization Credentials of a Requestor.
* **Authorization** - A process for approving or denying disclosure non-public registration data.
* **Credential**
	+ **"Identifier Credential":** A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in Validating an identity claimed by an entity that attempts to access a system. Example: [Username/Password], [OpenID credential], X.509 public-key certificate.
	+ **"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.
* **De-accreditation of Accreditation Authority –** An administrative action by which ICANN org revokes the agreement with the accreditation authority following which it is no longer approved to operate as the accreditation authority.
* **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.
* **Revocation of User Credentials-** The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.
* **Validate -** To test or prove the soundness or correctness of a construct.  (Example: The Discloser will Validate the Identity Credential and Authorization Credentials as part of its Authorization process.)
* **Validation -** Establish the soundness or correctness of a construct.
* **Verify -** To test or prove the truth or accuracy of a fact or value. (Example: Identity Providers Verify the identity of the requestor prior to issuing an Identity Credential.)
* **Verification -** The process of examining information to establish the truth of a claimed fact or value.

The EPDP Team recommends that a policy for accreditation of SSAD users is established.

The following principles underpin the accreditation policy:

1. SSAD must only accept requests for access/disclosure from accredited organizations or individuals. However, accreditation requirements must accommodate any intended user of the system, including an individual or organization who makes a single request. The accreditation requirements for regular users of the system and a one-time user of the system may differ.
2. Both legal persons and/or individuals are eligible for accreditation. An individual accessing SSAD using the credentials of an accredited entity warrants that the individual is acting on the authority of the accredited entity.
3. The accreditation policy defines a single Accreditation Authority, run and managed by ICANN org. This Accreditation Authority may work with external or third-party Identity Providers that could serve as clearinghouses to Verify identity and authorization information associated with those requesting accreditation.
4. 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, ICANN, or whatever authorization provider the EPDP Team ultimately agrees on.

Benefits of Accreditation:

1. Verifying the Identity of the Requestor:  The Accreditation Authority MUST verify the identity of the requestor, resulting in an Identity Credential.
2. 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, performed by an Identity Provider, results in Authorization Credentials. Authorization Credentials convey information such as:
	* Assertion as to the purpose(s) of the request
	* Assertion as to the legal basis of the requestor
	* Assertion that the user identified by the Identity Credential is affiliated with the Accreditation Authority
	* 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.
	* Assertions specific to the requestor – trademark ownership/registration for example
	* Power of Attorney statements, when/if applicable.
3. Validation of Identity Credentials and Authorization Credentials, in addition to the information contained in the request, facilitate the decision of the authorization provider to accept or reject the Authorization of an SSAD request. For the avoidance of doubt, the presence of these credentials alone DOES NOT result in or mandate an automatic access / disclosure authorization. However, the ability to automate access/disclosure authorization decision making is possible under certain circumstances.
4. Defines a base line “code of conduct” that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR - for the ICANN community, including:
	* A clear and concise explanatory statement.
	* A defined scope that determines the processing operations covered (the focus for SSAD would be on the Disclosure operation.)
	* Mechanism that allow for the monitoring of compliance with the provisions.
	* Identification of an Accreditation Body Auditor (a.k.a. monitoring body) and definition of mechanism(s) which enable that body to carry out its functions.
	* Description as to the extent a “consultation” with stakeholders has been carried out.
	* Etc.

The accreditation authority:

1. MUST have a uniform baseline application procedure and accompanying requirements for all applicants requesting accreditation, including:
	* Definition eligibility requirements for accredited users
	* Identity Validation, Procedures
	* Identity Credential Management Policies:  lifetime/expiration, renewal frequency, security properties (password or key policies/strength), etc.
	* Identity Credential Revocation Procedures: circumstances for revocation, revocation mechanism(s), etc.  [see also “Accredited User Revocation & abuse section below]
	* Authorization Credential Management: lifetime/expiration, renewal frequency, etc.
	* NOTE: requirements beyond the baseline listed above may be necessary for certain classes of requestors.
2. MUST define a dispute resolution and complaints process.
3. MUST be audited by an auditor on a regular basis. Should the Accreditation Authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to address the breach, but in cases of repeated failure, a new Accreditation Authority must be identified or created. Additionally, accredited entities MUST be audited for compliance with the accreditation policy and requirements on a regular basis; (Note: detailed information regarding auditing requirements can be found in the Auditing preliminary recommendation).
4. MAY develop user groups / categories to facilitate the accreditation process as all requestors will need to be accredited, and accreditation will include identity verification.
5. MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked and information about the identity providers it is working with.

Accredited User Revocation & Abuse:

1. Revocation, within the context of the SSAD, means the Accreditation Authority can revoke the accredited user’s status as an accredited user of the SSAD. A non-exhaustive list of examples where revocation may apply include 1) the accredited user’s violation of the code of conduct, 2) the accredited user’s abuse of the system, 3) a change in affiliation of the accredited user, or 4) where prerequisites for accreditation no longer exist.
2. A mechanism to report abuse committed by an accredited user must be provided by SSAD. Reports must be relayed to the Accreditation Authority for handling.
3. 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 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.
4. Revocation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Authority.

De-authorization of Identity Providers

1. The authorization policy for Identity providers should include graduated penalties. In other words, not every violation of the policy will result in De-authorization; however, De-authorization may occur if it has been determined that the Identity Provider has materially breached the conditions of its contract and failed to cure based on: a) a third-party complaint received; b) results of an audit or investigation by the Accreditation Auditor or auditor;  c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. Depending upon the nature and circumstances leading to the de-authorization of an Identity Provider, some or all of its outstanding credentials may be revoked or transitioned to a different Identity Provider.

Accredited entities or individuals:

1. MUST agree to:
	* only use the data for the legitimate and lawful purpose stated;
	* the terms of service, in which the lawful uses of data are described;
	* prevent abuse of data received;
	* [cooperate with any audit or information requests as a component of an audit;]
	* be subject to de-accreditation if they are found to abuse use of data or accreditation policy / requirements;
	* store, protect and dispose of the gTLD registration data in accordance with applicable law;
	* only retain the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.
2. Will not be restricted in the number of SSAD requests that can be submitted at a time, except where the accredited entity poses a demonstrable threat to the SSAD. It is understood that possible limitations in SSAD’s response capacity and speed may apply. For further details see the response requirements preliminary recommendation.

Fees:

The accreditation service should be part of a cost-recovery system. For further details, see the financial sustainability preliminary recommendation.

**Implementation Guidance**

In relation to accreditation, the EPDP Team provides the following implementation guidance:

1. Recognized, applicable, and well-established organizations could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting must take place if any such reputable and well-established organizations are to collaborate with the Accreditation Authority.
2. Examples of additional information the Accreditation Authority or Identity Provider may require an applicant for accreditation to provide could include:
	* a business registration number and the name of the authority that issued this number (if the entity applying for accreditation is a legal person);
	* information asserting trademark ownership.

Auditing / logging by Accreditation Authority and Identity Providers

1. The accreditation/verification activity (such as accreditation request, information on the basis of which the decision to accredit or verify identity was made) will be logged by the Accreditation Authority and Identity Providers.
2. Logged data shall only be disclosed, or otherwise made available for review, by the Accreditation Authority or Identity Provider, where disclosure is considered necessary to a) fulfill or meet an applicable legal obligation of the Accreditation Authority or Identity Provider; b) carry out an audit under this policy or; c) to support the reasonable functioning of SSAD and the accreditation policy.

See also auditing and logging preliminary recommendations for further details.

1. **Accreditation of entities carrying out a public policy task**

[TBC – proposed language to be provided by GAC team members]

1. **Criteria and Content of Requests**

The EPDP Team recommends that each SSAD request must include, at a minimum, the following information:

1. Domain name pertaining to the request for access/disclosure;
2. Identification of and information about the requestor (including, requestor’s accreditation status, if applicable, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
3. Information about the legal rights of the requestor specific to the request and specific rationale and/or justification for the request, (e.g., What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data?);
4. Affirmation that the request is being made in good faith and that data received (if any) will be processed lawfully and only in accordance with the justification specified in (c);
5. A list of data elements requested by the requestor, and why the data elements requested are adequate, relevant and limited to what is necessary.

The objective of this recommendation is to allow for the standardized submission of requested data elements, including any supporting documentation.

1. **Third Party Purposes/Justifications**

[As identified in the preliminary recommendation relating to criteria and content of requests, each request must include information about the legal rights of the requestor specific to the request and/or specific rationale and/or justification for the request, e.g. What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data? The EPDP Team expects that over time, the entity responsible for receiving requests will be able to identify certain patterns that could result in the development of a preset list of rationales and/or justifications that a requestor can select from, while always maintaining the option for the requestor to provide this information in free form”.]

1. **Receipt of acknowledgement**

The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, the response time for acknowledging receipt of a SSAD request should be without undue delay, but not more than two (2) business days from receipt, unless (i) shown circumstances do not make this possible or (ii) the SSAD is implemented using technologies which allow instantaneous responses to disclosure requests, in which case, the acknowledgement of receipt must be instantaneous.

Central Gateway Manager preliminary recommendation #3, criteria and content of request, Central Gateway Manager Central Gateway Manager

The response provided by the Central Gateway Manager should also include information about the subsequent steps as well as the timeline consistent with the recommendations outlined below.

1. **Contracted Party Authorization**
2. 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.
3. If deemed desirable, the Contracted Party may outsource the authorization responsibility to a third party provider, but the Contracted Party will remain responsible for ensuring that the applicable requirements are met.
4. While the requestor will have the ability to identify the lawful basis under which it expects the Contracted Party to disclose the data requested, the Contracted Party must make the final determination of the appropriate lawful basis for the Contracted Party to disclose the requested information.
5. The Contracted Party should make a threshold determination (without processing the underlying data) about whether the requestor has established an interest in the disclosure of personal data. The determination should consider the elements:
	* Is the identity of the requestor clear/verified?
	* Has the requestor provided a legitimate interest or other lawful basis in processing the data?
* Are the data elements requested necessary to the requestor’s stated purpose?
	+ Necessary means more than desirable but less than indispensable or absolutely necessary.
* Using the guidance provided in Preliminary Recommendation 3 (User Groups) and/or 5 (Purposes) about the usefulness and necessity of data elements, the authorization provider should determine whether the data elements requested are limited and reasonable to achieve the requestor’s stated purpose?
	+ Each request should be evaluated individually (i.e. each submission should contain a request for data related to a single domain. If a submission relates to multiple domains, each must be evaluated individually.).
	+ In addition, each data element in a request should be evaluated individually.

If the answer to any of the above questions is no, the Contracted Party may deny the request, or require further information from the requestor before proceeding to paragraph 6 below.

1. The Contracted Party may evaluate the underlying data requested once the validity of the request is determined under paragraph 4 above. The purpose of paragraph 5 is to determine whether the paragraph 6 [meaningful human review] is required. The Contracted Party’s review of the underlying data should assess at least:
* Does the data requested contain personal data?
	+ If no personal data, no further balancing required.
* 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.
	1. The Contracted Party should evaluate at least the following factors to determine whether the legitimate interest of the requestor is not outweighed by the interests or fundamental rights and freedoms of the data subject. No single factor is determinative; instead the authorization provider should consider the totality of the circumstances outlined below:
* **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[[4]](#footnote-4) for the data subject affected, this shall be taken into account during the decision-making.
* ​***Nature of the data***. Consider the level of sensitivity of the data as well as whether the data is already publicly available.
* ***Status of the data subject***. Consider whether the data subject’s status increases their vulnerability (e.g., children, other protected classes)
* ​***Scope of processing***. Consider information from the disclosure request or other relevant circumstances that indicates whether data will be [securely] held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk), .[provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS].
* ***Reasonable expectations of the data subject***. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.
* ​***Status of the controller and data subject***. Consider negotiating power and any imbalances in authority between the controller and the data subject.
* ***Legal frameworks involved***. Consider the jurisdictional legal frameworks of the requestor, Contracted Party/Parties, and the data subject, and how this may affect potential disclosures.

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.

If, based on consideration of the above factors, the Contracted Party determines that the requestor’s legitimate interest is outweighed by the interests or fundamental rights and freedoms of the data subject, the request may be denied. The rationale for the denial MUST be documented and MUST be communicated to the requestor, with care taken to ensure that no personal data is revealed to the requestor within this explanation.

1. The application of the balancing test and factors considered in paragraph 6 should be revised as appropriate to address applicable case law interpreting GDPR, guidelines issued by the EDPB or revisions to GDPR that may occur in the future.

**Implementation Guidance**

1. As noted in paragraph 4 above, in situations where the requestor has provided a legitimate interest for its request for access/disclosure, the Contracted Party should consider the following:
* Interest must be specific, real, and present rather than vague and speculative.
* An interest is generally legitimate so long as it can be pursued consistent with data protection and other laws.
* Examples of legitimate interests include: (i) enforcement of legal claims; (ii) prevention of fraud and misuse of services; and (iii) physical, IT, and network security.
1. **Authorization for automated disclosure requests**

For disclosure requests for which the steering committee (see below) has determined that these can be responded to in an automatic fashion the following requirements will apply:

1. The centralized gateway manager MUST confirm that all required information as per [building block a) ‘criteria and content of requests’](https://docs.google.com/document/d/1bl7GY496uqJ93TIC-39PLB22ZVP0ecW0Bdo91jk1UDI/edit) is provided and that the request meets the criteria established by the steering committee to qualify as an automated disclosure request.
2. 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.
3. A response is provided consistent with the SLAs outlined in preliminary recommendation #[X].
4. **Response Requirements**

For the Central Gateway Manager:

1. Following receipt of a disclosure request, the Central Gateway Manager must confirm[[5]](#footnote-5) that all required information as per the preliminary recommendation ‘criteria and content of requests’ is provided. Should the Central Gateway Manager establish that the request is incomplete, the Central Gateway Manager must provide an opportunity for the requestor to amend and resubmit its request.
2. Following confirmation that the request is syntactically correct and that all required information has been provided, the Central Gateway Manager must immediately and synchronously respond with an acknowledgement response and relay the disclosure request to the responsible contracted party, if it does not concern a request that meets the criteria for automatic disclosure.

For Contracted Parties:

1. The Contracted Parties 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.
2. Responses where disclosure of data (in whole or in part) has been denied should include: rationale sufficient for the requestor to understand the reasons for the decision, including, for example, an analysis and explanation of how the balancing test was applied (if applicable). Additionally, in its response, the entity receiving the access/disclosure request must include information on how public registration data can be obtained.
3. 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 EPDP Team recommends that if the Contracted Party determines that disclosure would be in violation of applicable laws or result in inconsistency with these policy recommendations, the Contracted Party must document the rationale and communicate this information to the requestor and ICANN Compliance (if requested).

If a requestor is of the view that its request was denied erroneously, a complaint should 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.

Implementation Guidance:

1. The Central Gateway Manager must confirm that the request is syntactically correct, including proper and valid Authentication and Authorization Credentials. Should the Central Gateway Manager establish that the request is syntactically incorrect, the Central Gateway Manager must reply with an error response to the requestor detailing the errors that have been detected.
2. Should the Central Gateway Manager establish that the request is incomplete, Central Gateway Manager must reply with an incomplete request response to the requestor detailing which data required by policy is missing, providing an opportunity for the requestor to amend its request.
3. Typically the acknowledgement response will include a “ticket number” or unique identifier to allow for future interactions with the SSAD.
4. An example of online critical infrastructure includes root servers; an example of offline critical infrastructure includes bridges. [examples to be provided by the EPDP Team]

**Implementation Guidance:** **Determining Variable SLAs for SSAD**

**How is priority defined?**

Priority is a code assigned to requests for disclosure that contain agreed to, best effort target response times. The spectrum of codes are 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.

**Who sets the priority?**

The initial priority of a disclosure request is set by the Central Gateway Manager based on the criteria outlined below.

**What happens if priority needs to be shifted?**

It is possible that the initially-set priority may need to be reassigned during the review of the request. For example, as a request is manually reviewed, the Central Gateway Manager and/or the Contracted Party may note that although the priority is set as 2 (UDRP/URS), the request shows no evidence documenting a filed UDRP case, and accordingly, the request should be recategorized as Priority 3. Any recategorization SHALL be communicated to the Requestor. The disclosing entity shall provide the requested information or provide a reason why it cannot disclose the information under the below-defined SLAs. It’s expected that the process and procedures based on best practices such as incident or problem management will ultimately govern the processing of disclosure requests and in particular the assignments and subsequent management of the assigned priority. An appeal mechanism will likely be required.

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, an appeal can be raised with the SSAD Steering Committee.

**Priority Matrix for non-automated disclosure requests**

| **Request Type** | **Priority** | **Proposed SLA (for discussion) / Compliance at 6 months / 12 months / 18 months** |
| --- | --- | --- |
| Urgent Requests“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.”  | 1 | 1 business day / 85% / 90% / 95% |
| Court orders, administrative proceedings (response to UDRP or URS filing, for example), etc.  | 2 | 2 business days / 85% / 90% / 95%*Note: this SLA is a current contractual obligation for registrars under the UDRP Rules (UDRP Rule 4(b))* |
| All other requests\* | 3 | 5 business days / 85% / 90% / 95% |

\*Note: Nothing in these policy recommendations explicitly prohibits the development of new categories and defined SLAs.

SLAs for automated requests are expected to be further developed during the implementation phase but these are expected to be under 60 seconds.

The EPDP Team recommends that, the SSAD Steering Committee will meet at least once per year or upon the occurrence of Triggering Event\* to revisit and revise, as appropriate, the above-defined SLA matrix.

In the event the SSAD Steering Committee identifies categories of requests that could be fully automated, e.g., notification of UDRP, the SSAD must allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are yet to be determined. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.

\*Triggering event to be defined by the EPDP Team

The "SSAD Steering Committee" means the group whose membership has been tasked with to reviewing and revising, as appropriate, the above-defined SLA matrix. The membership of the SSAD Steering Committee shall be made up of a representative body of ICANN community volunteers (see recommendation #17 below).

1. **Acceptable** **Use Policy**

The EPDP Team recommends that the following requirements are applicable to the requestor and must be confirmed by the Central Gateway Manager and subject to an enforcement mechanism. For the avoidance of doubt, every request does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.

The requestor:

1. Must only request data from the current RDS data set (no historic data);
2. Must, for each and every unique request for RDS data, provide representations of the corresponding purpose and lawful basis for the processing, which will be subject to auditing (see the auditing preliminary recommendation for further details);
3. MAY request data from the SSAD for multiple purposes per request, for the same set of data requested;
4. For each stated purpose must provide (i) representation regarding the intended use of the requested data and (ii) representation that the requestor will only process the data for the stated purpose(s). These representations will be subject to auditing (see auditing preliminary recommendation further details);
5. Must handle the data subject’s personal data in compliance with applicable law (see auditing preliminary recommendation for further details).

The EPDP Team recommends that the following requirements are applicable to Contracted Parties and subject to ICANN Compliance enforcement, as well as any automated responses provided by SSAD. For the avoidance of doubt, every response does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.

Contracted Parties and SSAD:

1. Must only disclose the data requested by the requestor;
2. Must return current data or a subset thereof in response to a request (no historic data);
3. Must process data in compliance with applicable law;
4. Must log requests;
5. Where required by applicable law, must perform a balancing test before processing the data;
6. Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per applicable law;
7. Where required by applicable law, must provide mechanism under which the data subject may exercise its right to erasure;
8. Confidentiality of disclosure requests – Data controllers of RDS data must make it clear to data subjects the types of entities/third parties which may process their data. Upon a request from a data subject the exact processing activities of their data within the SSAD, should be disclosed as soon as reasonably feasible. However the nature of legal investigations or procedures may require SSAD and/or the disclosing entity keep the nature or existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority, [and] [or] in accordance with the data subject's rights under applicable law.[[6]](#footnote-7)
9. **Query Policy**

The EPDP Team recommends that the Central Gateway Manager:

1. Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system;
2. May take measures to limit the number of requests that are submitted by the same requestor if it is demonstrated that the requests are of an abusive\* nature;

\*“Abusive” use of SSAD may include (but is not limited to) the detection of one or more of the following behaviors/practices:

1. High volume automated submissions of malformed or incomplete requests.
2. High volume automated duplicate requests that are frivolous or vexatious.
3. Use of false, stolen or counterfeit credentials to access the system.
4. Storing/delaying and sending high-volume requests causing the SSAD or other parties to fail SLA performance. When investigating abuse based on this specific behavior, the concept of proportionality should be considered.

As with other access policy violations, abusive behavior can ultimately result in suspension or termination of access to the SSAD. In the event the entity receiving requests makes a determination based on abuse to limit the number of requests a requestor, further to point b, the requestor may seek redress via ICANN org if it believes the determination is unjustified. For the avoidance of doubt, if the entity receiving requests receives a high volume of requests from the same requestor, the volume alone must not result in a de facto determination of system abuse.

1. MUST respond only to requests for a specific domain name for which non-public registration data is requested to be disclosed and MUST examine each request on its own merits.

The EPDP Team recommends the SSAD, in whatever form it eventually takes, MUST:

1. Unless otherwise required or permitted, not allow bulk access, wildcard requests, [reverse lookups[[7]](#footnote-8)], nor boolean search capabilities.
2. Have the capacity to handle the expected number of requests in alignment with the SLAs established
3. Only return current data (no data about the domain name registration’s history);
4. Receive a specific request for every individual domain name (no bulk access);
5. Direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data.

Requests must only refer to current registration data (historical registration data will not be made available via this mechanism).

1. **Terms of use**

The EPDP Team recommends that appropriate agreements, such as terms of use for the SSAD, a privacy policy and a disclosure agreement are put in place that take into account the recommendations from the other preliminary recommendations. These agreements are expected to be developed and negotiated by the parties involved in SSAD, taking the below implementation guidance into account.

Implementation guidance:

Privacy Policy

The EPDP recommends, at a minimum, the privacy policy shall include:

* Relevant data protection principles, for example,
* The type(s) of personal data processed
* How and why the personal data is processed, for example,
	+ verifying identity
	+ communicating service notices
* How long personal data will be retained
* The types of third parties with whom personal data is shared
* Where applicable, details of any international data transfers/requirements thereof
* Information about the data subject rights and the method by which they can exercise these rights
* Notification of how changes to the privacy policy will be communicated

Further consideration should be given during implementation whether updates to the RAA are necessary to ensure compliance with these recommendations.

Terms of Use

The EPDP recommends, at a minimum, the terms of use shall address:

* Indemnification of the disclosing party and ICANN.
* Data request requirements
* Logging requirements
* Ability to demonstrate compliance
* Applicable prohibitions

Disclosure agreements

The EPDP recommends, at a minimum, disclosure agreements shall address:

* Use of the data for the purpose indicated in the request
* Requirements for use of data for a new purpose other than the one indicated in the request
* Retention of data
* Lawful use of data
1. **Retention and Destruction of Data**

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. Requestors must retain only the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.

1. **Financial Sustainability**

The EPDP Team recommends that, in considering the costs and financial sustainability of SSAD, one needs to distinguish between the development and operationalization of the system and the subsequent running of the system.

The EPDP Team expects that the costs for developing, deployment and operationalizing the system, similar to the implementation of other adopted policy recommendations, to be initially borne by ICANN org, Contracted Parties and other parties that may be involved. It is the EPDP Team’s expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests.

The subsequent running of the system is expected to happen on a cost recovery basis whereby historic costs may be considered. For example, if the SSAD includes an accreditation framework under which users of the SSAD could become accredited, the costs associated with becoming accredited would be borne by those seeking accreditation. Similarly, some of the cost of running the SSAD may be offset by charging fees to the users of the SSAD.

When implementing and operating the SSAD, a disproportionately high burden on smaller operators should be avoided.

The EPDP Team recognizes that the fees associated with using the SSAD may differ for users based on [cost causation]. [awaiting proposed footnote from Brian K.]

[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.] <<Homework: (Amr, Brian, Stephanie & Franck) to clarify intent of statement; the statement intent is on-going maintenance/cost of the system; not to infer a blanket prohibition; (due Monday Jan 20)

The SSAD should not be considered a profit-generating platform for ICANN or the contracted parties. Funding for the SSAD should be sufficient to cover costs, including for subcontractors at market cost and to establish a legal risk fund. It is crucial to ensure that any payments in the SSAD are related to operational costs and are not simply an exchange of money for non-public registration data.

In relation to the accreditation framework:

1. Accreditation applicants may be charged a to-be-determined non-refundable fee proportional to the cost of validating an application.
2. Rejected applicants may re-apply, but the new application(s) may be subject to the application fee.
3. Fees are to be established by the accreditation authority.
4. Accredited users and organizations must renew their accreditation periodically.

**Implementation guidance**: (associated with disclosure requests):

[Given the number of policy options implicit in the various models, there are various implementation details that may have policy implications, particularly with respect to cost distribution and choice of party who performs various data protection functions. These issues are collected here under Implementation Guidance for consideration.] << suggestion by Stephanie

[The fee structure as well as the renewal period is to be determined in the implementation phase, following the principles outlined above. The EPDP Team recognizes that it may not be possible to set the exact fees until the actual costs are known. The EPDP Team also recognizes that the SSAD fee structure may need to be reviewed over time.

Placeholders

The EPDP Team will further consider whether the resubmission of a request will be treated as a new request from a cost/fee perspective.

The EPDP Team has requested input from ICANN Org concerning the expected costs of developing, operationalizing and maintaining the three different models. Based on the feedback received, the EPDP Team may develop further guidance in relation to the financial sustainability of SSAD. ]

1. **Automation**

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[[8]](#footnote-9). Additionally, in areas where automation is not both technically feasible and legally permissible, the EPDP Team recommends standardization as the baseline objective.

For example, the EPDP Team expects that aspects of the SSAD such as intake of requests, credential check, request submission validation (format & completeness, not content) could be automated, while it may not be possible to completely automate request review and disclosure.

The SSAD must allow for the automation of syntax checking of incoming requests, resulting in an automatic response that indicates the errors to the requestor. This automation addresses the risk of filling up the request queues of the discloser with malformed requests.

The SSAD must allow for the automation of checking that the contents of a request is complete, per policy, resulting in an automatic response that provides details explaining what elements are incomplete. This automation allows for the discloser to indicate - without human intervention - if any additional information is required per policy and enables the requestor to address the error.

The SSAD must allow for the automation of an immediate and synchronous response that indicates the receipt of a valid request and some indication that it will be processed. Typically, such responses include a "ticket number" or some kind of unique ID to allow for future queries (status, updates, deletion, etc.). This automation allows for efficient queue management on the discloser’s side and assists in ensuring the principal of "predictability" is met.

The SSAD must allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are yet to be determined. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.

1. **Logging**

The EPDP Team expects that the appropriate logging procedures are put in place to facilitate the auditing procedures outlined in these recommendations. These logging requirements will cover the following:

* Accreditation authority
* Central Gateway Manager
* Identity provider
* Activity of accredited users such as login attempts, queries
* What queries and disclosure decision(s) are made[[9]](#footnote-10)

The EPDP Team recommends:

1. The activity of all SSAD entities will be logged. (for further details, please see the implementation guidance below).
2. Logs will include a record of all queries and all items necessary to audit any decisions made in the context of SSAD.
3. Logs must be retained for a period sufficient for auditing and complaint resolution purposes, taking into account statutory limits related to complaints against the controller.
4. Logs must be retained in a commonly used, structured, machine-readable format accompanied by an intelligible description of all variables.
5. Logged data will remain confidential and must be disclosed in the following circumstances:
	1. In the event of a claim of misuse, logs may be requested for examination by an accreditation authority or dispute resolution provider.
	2. Logs should be further available to data protection authorities, ICANN, and the auditing body.[[10]](#footnote-11)
	3. When mandated as a result of due legal process, including relevant supervisory authorities, as applicable.
	4. General technical operation to ensure proper running of the system.

Implementation guidance:

At a minimum, the following events must be logged

* Logging related to the Identity Provider
	+ Details of incoming requests for Accreditation
	+ Results of processing requests for Accreditation, e.g., issuance of the Identity Credential or reasons for denial
	+ Details of Revocation Requests
	+ Indication when Identity Credentials and Authorization Credentials have been Validated.
* Logging related to the Central Gateway Manager
	+ Information related to the contents of the query itself.
	+ Results of processing the query, including changes of state (e.g., received, pending, in-process, denied, approved, approved with changes)
* Logging related to the entity Authorizing the request
	+ Request Response details, e.g., Reason for denial, Notice of approval and data elements released.
1. **Audits**

The EPDP Team expects that the appropriate auditing processes and procedures are put in place to ensure appropriate monitoring and compliance with the requirements outlined in these recommendations.

As part of any audit, the auditor MUST be subject to reasonable confidentiality obligations with respect to proprietary processes and personal information disclosed during the audit.

More specifically:

**Audits of the Accrediting Authority**

If ICANN outsources the accreditation authority function to a qualified third party, the accrediting authority MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the accreditation authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new accreditation authority must be identified or created.

Any audit of the accreditation authority shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data, and other information requested.

As part of such audits, the accreditation authority shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any [policy] breaches, noting that in such an extreme case, requirements for other entities involved in SSAD may be temporarily lifted until a confirmed breach has been addressed.

[If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches of the accreditation policy, noting that in such an extreme case, the credentials issued during the time of the breach will be reviewed. Modalities of this review should be established in the implementation phase.] << Janis proposal

[…that any SSAD users accredited during the period of the breach need to have their access to SSAD temporarily suspended until the breach is addressed.] << Amr suggestion to proposal

[There needs to be a concept of causality and proportionality between the breach (eg size, how bad) and the consequences.] << Franck suggestion

Notes for clarity:

Who performs audit?

Who determines a breach?

Who is disclosing data?

Who plays what roles?

What data was disclosed improperly?

**Audits of Identity Provider(s)**

Identity Providers MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the Identity Provider be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new Identity Provider must be identified.

Any audit of an Identity Provider shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the Identity Provider shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

**Audits of Accredited Entities/Individuals**

Appropriate mechanisms must be developed in the implementation phase to ensure accredited entities’ and individuals’ compliance with the policy requirements as defined in the accreditation preliminary recommendation. These could include, for example, audits triggered by complaints, random audits, or audits in response to a self-certification or self-assessment. Should the accredited entity or individual be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure the matter should be referred back to the Accreditation Authority and/or Identity Provider, if applicable, for action.

Any audit of accredited entities/individuals shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the accredited entity/individual shall, in a timely manner, provide to the auditor all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

**Audits of the Central Gateway Manager & Contracted Parties**

The EPDP Team will further consider these requirements once the EPDP Team has decided on the roles and responsibilities of the different parties in the SSAD.

NOTE: Depending on the ultimate SSAD model the EPDP Team recommends, there may be other relevant parties that would be subject to auditing. This will be revisited when the ultimate SSAD model is recommended.

[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.] << suggestion from Brian

**SSAD Implementation Guidance**

The EPDP Team recommends that, consistent with the preliminary recommendation that an SSAD request must be received for each domain name registration for which non-public registration is requested to be disclosed, it must be possible for requestors to submit multiple requests at the same time, for example, by entering multiple domain name registrations in the same request form if the same request information applies.

1. **SSAD Steering Committee**

In conjunction with the implementation of these recommendations, an SSAD Steering Committee is to be created. The SSAD Steering Committee will have the following responsibilities:

1. Review and revise, as appropriate, the SLA matrix;
2. Review and confirm which categories of disclosure requests must be automated (for example, local LE requests from a CP in jurisdiction);
3. Review and confirm other implementation improvements such as the identification of possible user categories and/or disclosure rationales;
4. Make recommendations to the GNSO Council for any policy issues that may require further policy work.

The SSAD Steering Committee shall consist of:

(i) Four individuals representing Contracted Parties appointed by the Contracted Party House;

(ii) One individual representing LE requestors appointed by the Governmental Advisory Committee;

(iii) One individual representing Intellectual Property requestors appointed by the Intellectual Property Constituency;

(iv) One individual representing business requestors appointed by the Business Constituency;

(v) One individual representing end-users and non-commercial users appointed jointly by the At-Large and the Non-Commercial Stakeholder Group;

vi) One individual representing security professionals appointed by the Security and Stability Advisory Committee (SSAC);

(vi) One liaison appointed by the Central Gateway Manager.

each appointed in accordance with the rules and procedures of the appointing organization; provided that such individuals should have direct experience and knowledge of SSAD.

The members of the SSAD Steering Committee commit to working in good faith towards the goals outlined in these policy recommendations.

Recommendations falling under a) – c) adopted by unanimity by the SSAD Steering Committee would be implemented immediately. Any recommendations falling under a) – c) not receiving unanimous support but having majority support of the steering committee members would be sent to the GNSO Council for confirmation by a GNSO Supermajority vote.

A detailed charter for the SSAD Steering Committee is expected to be developed during the implementation phase.

1. Some have suggested that the 30 day response time that is provided to controllers when a data subject requests for information about which of his/her personal data is being processed is reasonable, but it should be recognized that gathering such information may be a lot more cumbersome than assessing a request for disclosure to registration data which is readily available to the controller and more in line with the existing requirements for registrars in relation to UDRP contact information verification. [↑](#footnote-ref-1)
2. Note, for ease of reading, all comments provided on the preliminary recommendations have for now been removed. In preparation for the F2F meeting, the staff support team will add those comments in that have not been addressed as a result of this proposal and/or require further discussion. [↑](#footnote-ref-2)
3. Note that accreditation is not referring to accreditation/certification as discussed in GDPR Article 42/43. [↑](#footnote-ref-3)
4. [include reference to relevant GDPR provision] [↑](#footnote-ref-4)
5. It is the expectation that the initial review of the completeness of requests is done automatically with the system not accepting the request until all requested data has been provided. [↑](#footnote-ref-5)
6. The EPDP Team may reconsider this requirement once there is clarity on who will be the entity disclosing the data. [↑](#footnote-ref-7)
7. The EPDP Team is expected to request legal guidance on the issue of reverse lookups. Based on that input, this recommendation will be updated accordingly. [↑](#footnote-ref-8)
8. EPDP Team to revisit this language once the decision of who will be the authorization provider is made. [↑](#footnote-ref-9)
9. Note, EPDP Team to review at a later stage as the ability for SSAD to log this information depends on who is the entity that makes the disclosure decision [↑](#footnote-ref-10)
10. Note, EPDP Team to review at a later stage as there is a question of the set up of the system of whether or not the Ry and RR as Controllers (where liability remains with them) may require access to the logs for them to engage in audit, or answer Data Subject requests. [↑](#footnote-ref-11)