March 23, 2020

Ms. Marika Konings
Senior Director, Policy Development Support
ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Re: Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2

Dear Ms. Konings:

INTA is pleased to submit its responses to the recommendations issued by the EPDP in regard to the development and implementation of a legally compliant System for Standardized Access/Disclosure to non-public gTLD registration data (“SSAD”). We are encouraged to see that the working group has acknowledged intellectual property claims as a legitimate purpose for requesting registrant data and that an automated intake system is recommended.

We appreciate the hard work and intensive effort that led to these comprehensive recommendations. However, we feel that there is much work to be done. This is in light of the concerns expressed by governments and the private sector with regard to expeditious access to information that is critical to fighting domain abuse and cybercrime. Our specific recommendations include:

1. The EPDP should revisit the possibility of a completely centralized SSAD model in light of apparently inconsistent comments on this subject from data protection authorities and the legal guidance that ICANN has received;
2. Disclosure of registration data should be guaranteed where request criteria have been met;
3. Automated response to requests is only applicable from Day 1 to requests from law enforcement and in response to UDRP/URS providers for registrant verification in an active UDRP/URS proceeding; such automation should be expanded to cover additional Day 1 use cases including for well-founded allegations of IP infringement, phishing, fraud and other similar matters of consumer protection;
4. ICANN must fully address how it will ensure consistency in the application of disclosure request processing by individual Contracted Parties, if the proposed hybrid model is ultimately retained. Otherwise, the community will be left with a fragmented system with inconsistent disclosure decisions by individual registries and registrars with no mechanism for ensuring consistency and sufficiency of responses; and
5. GDPR specifically incorporates balance in terms of protecting privacy versus ensuring access to data for legitimate third-party purposes; any acceptable SSAD must go further in recognizing this, including in terms of (a) ensuring underlying data is accurate and up-
to-date (art. 5 of GDPR), (b) ensuring processors/controllers are applying any art. 6(1)(f) balancing test in good faith in recognition of the balance required under GDPR and in support of the legitimate third-party purposes identified in the SSAD proposal and EPDP Phase 1 report to which INTA commented; (c) enabling access to a certain degree of historical data and facilitating reverse correlation capability (i.e. reverse WHOIS/reverse Registrant Data Directory Service [RDDS]) to properly support third-party purposes; (d) recommending either general publication or automatic disclosure through SSAD of data not subject to the privacy protections of GDPR, including data of legal persons and where the data is otherwise not subject to GDPR on jurisdictional grounds (i.e. no party in the data flow is subject to EU law, including registrant and registrar/registry).

Thank you for your consideration of INTA’s comments. If you have any further questions or comments regarding this submission, please feel free to contact Lori Schulman, Senior Director, Internet Policy at lschulman@inta.org or +1(202)704-0408.

Sincerely,

Etienne Sanz de Acedo
Chief Executive Officer

About INTA

INTA is a global not-for-profit association with more than 7,200 member organizations from over 187 countries. One of INTA’s goals is the promotion and protection of trademarks as a primary means for consumers to make informed choices regarding the products and services they purchase. During the last two decades, INTA has also been the leading voice of trademark owners within the Internet community, serving as a founding member of the Intellectual Property Constituency of the Internet Corporation for Assigned Names and Numbers (ICANN). INTA’s Internet Committee is a group of over 175 trademark owners and professionals from around the world charged with evaluating treaties, laws, regulations and procedures relating to domain name assignment, use of trademarks on the Internet, and unfair competition on the Internet, whose mission is to advance the balanced protection of trademarks on the Internet.
EPDP On the Temporary Specification for gTLD Registration Data - Phase 2 - Public Comment Proceeding Input Form

1. Email address: lschulman@inta.org

Important Instructions - PLEASE READ BEFORE PROCEEDING

This Public Comment forum seeks community feedback on the Initial Report published by the Expedited Policy Development Process (EPDP) Team on the Temporary Specification for gTLD Registration Data.

This is a new format for collecting public comment. It seeks to:
-- Clearly link comments to specific sections of the initial report
-- Encourage commenters to provide reasoning or rationale for their opinions
-- Enable the sorting of comment so that the EPDP team can more easily read all the comments on any one topic

There is no obligation to complete all sections within this form -- respond to as many or as few questions as desired. Additionally, there is the opportunity to provide comments on the general content of the Initial Report or on new issues not raised by the Initial Report. To preview all questions in the Google Form, please refer to a Word version of this form here here's the link to the Word doc:
<INSERT NEW LINK>

As you review the "Questions for Community Input" in the Initial Report, you will note that there is not a 1:1 correspondence with the questions asked in the Public Comment format. This is because, in some instances, the "Questions for Community Input" have been divided into multi-part questions so that feedback on these questions would be clear. The Initial Report and Comment Forum have been reviewed to ensure that all the "Questions for Community Input" have been addressed in this Comment Forum.

It is important that your comments include rationale (i.e., by answering the "rationale" question in each section). This is not a vote. The EPDP team is interested in your reasoning so that the conclusions reached and the issues discussed by the team can be tested against the reasoning of others. (This is much more helpful than comments that simply "agree" or "disagree").

You can easily navigate from page to page in the form. There is a table of contents below so that you can "fast forward" to the desired section by hitting "next" at the bottom of each page. To preview this entire form in Word format, see the link to the Word doc:
<INSERT NEW LINK>

To stop and save your work for later, you MUST (to avoid losing your work):

1. Provide your email address above in order to receive a copy of your submitted responses;

2. Click "Submit" at the end of the Google Form (the last question on every page allows you to quickly jump to the end of the Google Form to submit);

3. After you click "Submit," you will receive an email to the above-provided email address; within the email, click the "Edit Response" button at top of the email;

4. After you click the "Edit Response" button, you will be directed to the Google Form to return and complete;
5. Repeat the above steps 2-4 every time you wish to quit the form and save your progress.

NOTES:
-- Please refer to the specific recommendation and relevant section or page number of the Initial Report for additional details and context about each recommendation. Where applicable, you are encouraged to reference sections in the report for ease of the future review by the EPDP Team.

-- Your comments should take into account scope of the EPDP as described by the Charter and General Data Protection Regulation (GDPR) compliance.

-- For transparency purposes, all comments submitted to the Public Comment forum will be displayed publicly via an automatically-generated Google Spreadsheet when the commenter hits the “Submit” button. Email addresses provided by commenters will not be displayed.

-- To maximize the visibility of your comments to the EPDP Team, please submit your comments via this form only. If you are unable to use this form, alternative arrangements can be made.

-- Please note you may encounter a character limit when submitting a response. In the event you encounter a character limit, you may send an email to policy-staff@icann.org, and the EPDP Support Staff will assist you with your response.

-- The final date of the public comment proceeding is 23:59 UTC on 23 March 2020. Any comments received after that date will not be reviewed / discussed by the EPDP Team.

Table of Contents

Page 1: Email Address, Important Instructions, Table of Contents
Page 2: Consent & Authorization
Page 3: EPDP Team Phase 2 Recommendations #1-7
Page 4: EPDP Team Phase 2 Recommendations #8-9
Page 5: EPDP Team Phase 2 Recommendations #10-16
Page 6: EPDP Team Phase 2 Recommendation #17
Page 7: EPDP Team Phase 2 Recommendations #18-19; Implementation Guidance i-ii
Page 8: Other Comments & Submission

Consent & Authorization
By submitting my personal data, I agree that my personal data will be processed in accordance with the ICANN Privacy Policy (https://www.icann.org/privacy/policy), and agree to abide by the website Terms of Service (https://www.icann.org/privacy/tos).

2. Please provide your name: * Lori S. Schulman

3. Please provide your affiliation * INTA
4. Are you providing input on behalf of another group (e.g., organization, company, government)? *
   Mark only one oval.

   ☐ Yes
   ☐ No

5. If yes, please explain: International Trademark Association (INTA)

   __________________________________________________________
   __________________________________________________________
   __________________________________________________________
   __________________________________________________________

Save Your Progress

6. Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.
   Mark only one oval.

   ☐ Yes Stop filling out this form.
   ☐ No, I would like to continue to the next section

Section 3, EPDP Preliminary Recommendations for Comment #1-7

This public comment proceeding seeks to obtain input on the Initial Report of the Phase 2 EPDP on the Temporary Specification for gTLD Registration Data Team. The Phase 2 EPDP Team is tasked with evaluating a System for Standardized Access/Disclosure to non-public gTLD registration data (“SSAD”).

Recommendation #1: Accreditation

Please find a link to the text of Recommendation 1 here:
https://docs.google.com/document/d/1Mq8T1EBcQhbKnCBcVwYtb3gKDIgJcOClu5G0NaNaO50/edit.

7. Please choose your level of support for Recommendation #1:
   Mark only one oval.

   ☐ Support Purpose as written
   ☐ Support intent with wording change
   ☐ Significant change required: changing intent and wording
   ☐ Purpose should be deleted
   ☐ No opinion
The INTA recommends the following revisions to the working definitions in Recommendation #1:

**Authentication** - The process or action of Validating the Identity Credential and Signed Assertions of a Requestor. [INTA notes that the term “Requestor” is not defined anywhere and appears inconsistently in initial cap or all lower case. Should be defined in this section. We suggest a specific definition for this term below.]

- **Authorization** - A process for approving or denying disclosure of non-public registration data.

- **De-accreditation of Accreditation Authority** – An administrative action by which ICANN org revokes the agreement with the accreditation authority, if this function is outsourced to a third party, following which it is no longer approved to operate as the accreditation authority. [Moved this definition to appear in alphabetical order.]

- **“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.

[We suggest reordering these definitions so they appear in alphabetical order.]

- **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 Signed Assertions 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 third parties.

- **Requestor** – An individual or organization seeking access to non-public domain name registration data through the SSAD.

- **Revocation of User Credentials** - The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.

- **Signed Assertion** - A data object that is a portable representation of the association between an Identifier Credential and one or more access assertions, and that can be presented for use in Validating those assertions for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate. [Moved to appear in alphabetical order.]

**INTA COMMENTS:**
The definitions have been only revised slightly and placed in alphabetical order but in general should be expanded significantly to include many additional terms used in the policy text below, as found in the EPDP Phase 2 Team working definitions available in the ICANN documents linked to the Initial Report. The EPDP Phase 2 team’s working definitions, which include draft definitions for terms such as “Legitimate Interest”, “Right of Access”, “Disclosure” would be helpful here. The above definitions appear to come from different sources and take different approaches to defining the components of the SSAD. Some have a legal context or approach (e.g., third parties, signed assertions), while others employ terms typically identified with automation, computing systems or even mathematics (e.g., data object, construct, a value, truth). Many employ terms treated as defined terms (e.g., “Requestor”, “Discloser”) that are
not defined here but should be. A proposed definition for Requestor has been inserted based on its use in other definitions above and incorporating the related terms from those definitions in which Requestor was used. It would also be useful to see how SSAD and these terms relate to the existing WhoIs system, perhaps making reference to data objects currently used (e.g., registrant, registrant organization) and how they would be accessed and disclosed under SSAD.

The EPDP Team recommends that a policy for accreditation of SSAD users is established. The following principles underpin the accreditation policy:

a) 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. [Comment: Any differences in such requirements should be provided by the EPDP along with rationale.]

b) Both legal entities and/or individuals are eligible for accreditation. An individual accessing SSAD using the credentials of an accredited entity (e.g. legal persons) warrants that the individual is acting on the authority of the accredited entity.  
[Comment: Are the individuals identified in the signed assertions or are the warranties separate documents or assertions?]

c) The Accreditation policy defines a single Accreditation Authority, 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.

d) The decision to authorize disclosure of non-public registration data, based on Validation of the Identity Credential, Signed Assertions, and data as required in preliminary recommendations concerning criteria and content of requests, will reside with the Registrar, Registry or the Central Gateway Manager, as applicable.  
[Comment: Are these delineated sufficiently in the referenced recommendations; is the decision resident with each of the contract parties listed separate or co-dependent. Need to clarify or link to the recommendations that show which aspects of the authorization decision reside with the Rr, which with the Ry and which with the CGM/ICANN. It should be clarified whether requests will initially be routed to the Rr or Ry or both, or responded to automatically by the CGM where possible.]

Requirements of the Accreditation Authority

e) Verifying the Identity of the Requestor: The Accreditation Authority MUST verify the identity of the Requestor, resulting in an Identity Credential.

f) Management of Signed Assertions: 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 a Signed Assertion.

g) Signed Assertions convey information such as:
   o Assertion as to the purpose(s) of the request
   oAssertion as to the legal basis of the Requestor
   o Assertion that the user identified by the Identity Credential is affiliated with the relevant organization [Comment: Is this one Requestor in which an individual is part of the Requestor due to the affiliation, e.g. an Authorized Representative, or are each of the individual and the entity authorized as separate Requestors? This should be clarified.]
- Assertion regarding compliance with laws (e.g., storage, protection and retention/disposal of data) [Comment: Will these be provided as standards agreed upon under GDPR or identified based on ICANN policy? Will it be a general assertion to comply with applicable laws or will there be more specific compliance requirements provided?]
- Assertion regarding agreement to use the disclosed data for the legitimate and lawful purposes stated [Comment: Will there be a standard set of warranties developed that apply to all users equally, or will there be distinctions based on entity versus individual, or some other status, such as private sector, government, law enforcement, etc.?]
- 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 status of the specific Requestor – trademark ownership/registration for example [Comment: Will documents or written evidence have to be submitted or are signed assertions sufficient?]
- Power of Attorney statements, when/if applicable. [Comment: when will such PoA statements be required/applicable? For any user acting on behalf of another party? Only for qualified legal counsel?]

h) Validation of Identity Credentials and Signed Assertion, in addition to the information contained in the request, to 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 where lawful. [Comment: What does this mean, under which circumstances and compliance with which law according to which decision maker? In which circumstances? For purposes of disclosure, INTA would strongly support automated or quasi-automated (i.e. human review by the central managing authority for provision of required info) access/disclosure decisions in cases of well-founded allegations of cybersquatting, trademark or copyright infringement, as evidenced in the assertions and supporting materials produced in connection with same/with the disclosure request itself. Other comments regarding automation are provided below.]

i) Defines a baseline “code of conduct”\(^\text{12}\) that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR, 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.)
- The mechanism that allows 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.

The Accreditation Authority:

j) MUST have a uniform baseline application procedure and accompanying
requirements for all applicants requesting Accreditation, including:
  o Definition of eligibility requirements for accredited users
  o Identity Validation Procedures
  o Identity Credential Management Policies: lifetime/expiration, renewal frequency, security properties (password or key policies/strength), etc.
    [Comment: INTA would prefer longer lifetime/periods for accreditation (subject to audit) and no/low cost accreditation / cost recovery model.]
  o Identity Credential Revocation Procedures: circumstances for revocation, revocation mechanism(s), etc. [see also “Accredited User Revocation & abuse section below]
  o Signed Assertions Management: lifetime/expiration, renewal frequency, etc.
  o NOTE: requirements beyond the baseline listed above may be necessary for certain classes of requestors.

k) MUST define a dispute resolution and complaints process to challenge actions taken by the Accreditation Authority.

l) MUST be audited by an auditor on a regular basis. [Comment: How often? This should be defined more specifically.] 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).

m) MAY develop user groups / categories to facilitate the accreditation process as all requestors will need to be accredited, and accreditation will include identity verification.

n) MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked, complaints received and information about the identity providers it is working with.

[Comment: As this section appears to be similar in summarizing the process and features addressed above the same comments apply regarding the need for clarification of standards and consistent use of terms to follow the process.]

Accredited User Revocation & Abuse:
  o) 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. [Comment: Per the comments above regarding the legal entity Requestor that has an affiliated individual, does a dissociation of one authorized representative automatically result in the revocation of an entity’s Accreditation? Presumably this would not be the case for the legal entity, but may be the case for the individual – but this should be clarified. In addition, we reiterate that what constitutes an abuse of the system and/or a code of conduct violation must be made explicit. How is abuse of the system defined? How does it differ from violating code of conduct? We would also suggest that the EPDP team provide further details regarding the development of a code of conduct, when and how that would take place, and whether it would be necessary to have a separate code of conduct or whether a code of conduct could be built in to the terms of use for the SSAD along with an acceptable use policy and privacy policy. Regardless, development of the
code of conduct / terms should involve all SSAD stakeholders.

p) 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.
[Comment: How will abuse be defined and what verification/validation process will be used to assure that a claim of abuse is valid, legitimate, etc.?]

q) The revocation policy for individuals/entities SHOULD include graduated penalties. In other words, not every violation of the system will result in Revocation; however, Revocation MAY occur if the Accreditation Authority determines that the accredited individual or entity has materially breached the conditions of its accreditation and failed to cure based on: a) a third-party verified complaint received; b) results of an audit or investigation by the Accreditation Authority or Accreditation Authority Auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy; e) results of audit or investigation by a DPA.

r) 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.

s) Revocation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Authority.
[Comment: There should be a defined appeals process for any revocation decisions.]

De-authorization of Identity Providers

t) 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.
[Comment: As there does not appear to be a process for “authorization” of an Identity Provider (which can be an Accreditation Authority), it may be helpful to clarify how that process would work to enable further comment on de-authorization of Identity Providers.

Accredited entities or individuals:

u) MUST agree to:
o only use the data for the legitimate and lawful purpose stated;
o the terms of service, in which the lawful uses of data are described;
o prevent abuse of data received;
o [cooperate with any audit or information requests as a component of an audit;] [Comment: What is the purpose of bracketed materials, are these subject to change or interim provisions? The brackets should be removed – INTA would support the inclusion of this item.]
o be subject to de-accreditation if they are found to abuse use of data or accreditation policy / requirements;
o store, protect and dispose of the gTLD registration data in accordance with applicable law;
o only retain the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.

v) Will not be restricted in the number of SSAD requests that can be submitted during a specific period of time, except where the accredited entity or individual 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. [Comment: Additional clarification for what would constitute a “demonstrable threat” to the SSAD should be provided.]

Fees:
The accreditation service will be a service that is financially sustainable. For further details, see the financial sustainability preliminary recommendation.

Implementation Guidance

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

a) Recognized, applicable, and well-established organizations could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting, as described in j) above, MUST take place if any such reputable and well-established organizations are to collaborate with the Accreditation Authority.

b) Examples of additional information the Accreditation Authority or Identity Provider MAY require an applicant for accreditation to provide could include:
o a business registration number and the name of the authority that issued this number (if the entity applying for accreditation is a legal person);
o information asserting trademark ownership. [Comment: This could be clarified – does this refer to information demonstrating ownership of a trademark by the accredited party or that the accredited party is acting on behalf of a trademark owner (or both)? What kinds of information would this entail? Copy of TM registration / certificate? Power of Attorney or other form demonstrating agency?]

INTA COMMENTS:

In general, INTA supports the concept of requiring additional information regarding standard and readily available electronic data regarding the active status of a trademark registration, but rights holders with valid claims to ownership or the establishment of rights based on pending applications, judicial recognition, or other evidence of common law trademark rights should not be summarily prohibited from qualifying for Accreditation through
verifiable accepted means relied upon in their home jurisdiction as a basis for sustaining such rights. INTA looks forward to specific provisions that embody the concepts for additional information requirements noted in Implementation Guidance subsection b) above.

Auditing / logging by Accreditation Authority and Identity Providers

c) 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.

d) 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.

**Recommendation #2: Accreditation of governmental entities**

Please find a link to the text of Recommendation #2 here: [https://docs.google.com/document/d/1NOTbh3PeQSaDr3C4GKjGjJPHgpB3bVIMTyJvz7pzpsU/edit](https://docs.google.com/document/d/1NOTbh3PeQSaDr3C4GKjGjJPHgpB3bVIMTyJvz7pzpsU/edit)

9. Choose your level of support of Recommendation #2:

   Mark only one oval.

   - [ ] Support Recommendation as written
   - [x] Support Recommendation intent with wording change
   - [ ] Significant change required: changing intent and wording
   - [ ] Recommendation should be deleted
   - [ ] No opinion

10. If your response requires an edit or deletion of Recommendation #2, please indicate the revised wording and rationale here.

   - Objective of accreditation
     
     SSAD SHOULD [Comment: MUST] ensure reasonable access to RDDS for entities that require access to this data for the exercise of their public policy task. In view of their obligations under applicable data protection rules, the final responsibility for granting access to RDDS data will remain with the party that is considered as the controller for the processing of that RDDS data that constitutes personal data.

     Notwithstanding these obligations, the decisions that these data controllers will need to make before granting access to RDDS data to a particular entity, can be greatly facilitated by means of the development and implementation of an accreditation procedure. The accreditation procedure can provide data controllers with information necessary to allow them to assess and decide about the disclosure of data. [Comment: Is this any different than the accreditation procedure outlined above? Or would this section envision a separate channel for access for government entities (including LEA)?]

   - Eligibility
     Accreditation by a countries’/territories’ government body or its authorized body
Comment: What does this refer to? would be available to various eligible government entities that require access to non-public registration data for the exercise of their public policy task, including, but not limited to:

- Civil and criminal law enforcement authorities,
- Judicial authorities,
- Consumer rights organizations,
- Cybersecurity authorities, including national Computer Emergency Response Teams (CERTs),
- Data protection authorities

(f) Accreditation procedure
Accreditation would be provided by an approved accreditation authority. This authority may be either a countries'/territories' governmental agency (e.g. a Ministry) or delegated to an intergovernmental agency. This authority SHOULD [Comment: MUST] publish the requirements for accreditation and carry out the accreditation procedure for eligible government entities.

- The accreditation authority reserves the right to update what credentials or other material are required for accreditation. [Comment: Which shall not go into effect until the current accreditation period is up for renewal.]

a. Renewal
Accredited/authenticated parties MUST renew their accreditation/authentication periodically. Each accreditation authority SHOULD determine an appropriate time limit. [Comment: Should this not be uniform for all accredited entities? If not, why not?]

B. Data access
- Accreditation is required for a party to participate in the access system (SSAD). Unaccredited parties can make data requests outside the system, and contracted parties should have procedures in place to provide reasonable access. [Comment: These should be required to be at least equivalent to Temp Spec reasonable access requirements and SLAs.]
- Accreditation does not guarantee disclosure of the data. The final responsibility for the decision to disclose data lies with the data controller.
- Any accredited user will be expected to only process the personal data that it needs to process in order to achieve its processing purposes. They will be obligated to minimize the number of queries they make to those that are reasonably necessary to achieve the purpose.
- Accredited entities will be required to follow the safeguards as set by the disclosing system.
- Disclosure of RDDS data to the type of third parties MUST be made clear to the data subject. Upon a request from a data subject inquiring about the exact processing activities of their data within the SSAD, relevant information 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 in
accordance with the data subject's rights under applicable law. [Comment: There must be defined mechanisms to rectify improper disclosure by accrediting entity or controller of the existence or nature of a confidential disclosure request.]

Please delete this: [In view of their obligations under applicable data protection rules, the final responsibility for granting access to RDDS data will remain with the party that is considered as the controller for the processing of that RDDS data that constitutes personal data.]

**Rationale:** It implies that the decision to disclose is solely at the controller's discretion, even if disclosure would otherwise be required under the policy. It is also inconsistent with other sections of the policy (such as the automation recommendations) that require automated disclosure in certain circumstances.

**Also – please add the following for clarity:**
[This recommendation is intended to apply to governmental bodies at all levels, such as local municipalities, cities, states, and provinces, in addition to countries and territories.]

---

**Recommendation #3: Criteria and Content of Requests**

Please find a link to Recommendation #3 here: [https://docs.google.com/document/d/1_w7EJHo4RzPtRis-zKgyJ4GzmY3KvQjk-o03n7Yuzk/edit](https://docs.google.com/document/d/1_w7EJHo4RzPtRis-zKgyJ4GzmY3KvQjk-o03n7Yuzk/edit).

11. **Choose your level of support of Recommendation #3:**

   *Mark only one oval.*

   - Support Recommendation as written
   - **Support Recommendation intent with wording change**
   - Significant change required: changing intent and wording
   - Recommendation should be deleted
   - No Opinion
Revised page 13

12. If your response requires an edit or deletion of Recommendation #3, please indicate the revised wording here.

On sub-section (b) – It is assumed that, for the sake of efficiency, such identification and information will be automated once the requestor has input its accreditation credentials and that the requestor will not be asked to manually input such identification and information for each request.

On sub-section (c) – information about the legal rights of the requestor and rationale for request – a threshold should be set, probably a relatively low one, in order to avoid lengthy requests and the need to present the full legal case solely for the purpose of obtaining the data and on the other hand to have a minimal standard that must be met. Much of this can likely be accomplished by the use of check-box selections covering the most common types of legal rights, request rationale, etc.

On sub-section (f) – self designation of the request type should not be the absolute criteria since this is likely to be misused. While the categorization by the requestor can be taken into account, it cannot be the decisive factor. Possibly the centralized system can designate certain priority levels depending on the nature of the request, e.g. criminal issues will be top priority while civil claims that do not involve imminent public harm would not be classified as urgent by default.

It is noted that supporting documentation may be submitted. To the extent that the documentation is not in English, it should be provided which languages are acceptable and which ones require attaching an English translation. In addition, it should be determined what type of translation would be acceptable – any translation, certified translation etc.

Recommendation #4: Third Party Purposes/Justifications

Please find a link to Recommendation #4 here: https://docs.google.com/document/d/1Xrx96CiQMhMff-dmCQWtomZ_ATISz9gRBSm72z0bzTA/edit?usp=sharing.

13. Choose your level of support of Recommendation #4:

Mark only one oval.

☐ Support Recommendation as written
☐ Support Recommendation intent with wording change
☐ Significant change required: changing intent and wording
☐ Recommendation should be deleted
☐ No Opinion

14. If your response requires an edit or deletion of Recommendation #4, please indicate the revised wording and rationale here.

Recommendation #5: Acknowledgement of receipt
Please find a link to Recommendation #5 here: https://docs.google.com/document/d/140U4AsH3so8tSojhdCEUa8I2QkD8OwBXxK9NclijCx4/edit?usp=sharing

15. Choose your level of support of Recommendation #5:

Mark only one oval.

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No opinion

16. If your response requires an edit or deletion of Recommendation #5, please indicate the revised wording and rationale here.

A more specific timeframe for acknowledgment of receipt should be set, if such is to be manual, for instance 24 hours. Alternatively, it can be automated and in such case almost immediate, similar to other technological ticketing systems.

Likewise, a timeframe should be set for provision of additional information by the requestor if the Central Gateway Manager determines that a request submitted is incomplete. Three business days could be a feasible timeframe for rectification of such incomplete request.

“The Central Gateway Manager MUST confirm that all required information as per preliminary recommendation #3, criteria and content of request, is provided.” [Comment: Change to active voice: The Central Gateway Manager MUST confirm that the requestor has provided all required information, criteria, and content of the request, as per preliminary recommendation #3.]

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.” [Comment: “with a response indicating that the request is incomplete…” Current wording makes it sounds like the CGM is sending an incomplete response. This should be revised to make the intended meaning more obvious.

**Recommendation #6: Contracted Party Authorization**

Please find a link to Recommendation #6 here: https://docs.google.com/document/d/1-iiPCpZMdpYmhpLzqbHHbG7NvlKt80-AbjPPj-isHnM/edit?usp=sharing.

17. Choose your level of support of Recommendation #6:

Mark only one oval.

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No opinion
18. If your response requires an edit or deletion of Recommendation #6, please indicate the revised wording and rationale here.

On sub-section (1) we recommend that further information be provided on instances where automated review would be used and in what cases automated disclosure may apply. The current wording is very vague on this point and requires further clarification along with examples of applicable scenarios. Also, this should more appropriately state “legally permissible and technically feasible” rather than “legally and technically permissible”.

On sub-section (2), we recommend further defining which third-party providers may be used by the Contracted Party and what criteria they should meet.

On sub-section (4), we strongly support that disclosure cannot be refused on the basis that there is no legal proceeding at the time since in many cases the information would be required in order to prepare the legal proceeding or determine the relevant party in such proceeding as part of the investigation preceding the actual legal proceedings. Pre-proceeding disclosures will also promote negotiated resolutions of disputes thus avoiding unnecessary filing of formal complaints. It is important to keep in mind always that in this context, we are talking about disclosing information relevant to an investigation or preparation of a legal claim – not prejudging (or asking a contracted party/data controller to prejudge) the merit of such investigation or claim.

In sub-section (5) it states that the “Contracted Party MAY evaluate the underlying data requested once the validity of the request is determined under bullet point #4 above”. This should be changed to a “MUST” and it could be clarified what “bullet point #4 refers to. In addition, use of the term “authorization provider” is unclear and we suggest for the sake of consistency referring to “Contracted Party” unless there is broader set of “authorization providers” evaluating the requests and if so, this should be clearly stated and defined.

In sub-section (5) “assessment of impact” should, in our opinion, encompass impact on all relevant parties and not solely on the data subjects, e.g. the requesting party, average consumers if applicable, etc.

In sub-section (5) “status of the data subject” it is unclear whether minors can register domain names. Even if so, further examples of “other protected classes” should be presented. In our opinion, this information would not necessarily be available to the Contracted Party and this criterion should be further considered.

In sub-section (5) it is not clear how “combined with other data” makes the scope of processing more high risk. Please elaborate on how combining data with other data increases the risk of data not being securely held; if you cannot provide a rationale for this assertion, this element of the recommendation should be deleted.

In sub-section (5) it states “Status of the controller and data subject. Consider negotiating power and any imbalances in authority between the controller and the data subject.” It is not clear how this is relevant when we know the disclosing party, under the proposed system, will be a registry operator or registrar. Please elaborate on why this was included and how it is relevant here.

In sub-section (5), it states “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." We would suggest that, based on this assessment, if no applicable law would prohibit disclosure, then disclosure should be mandatory.

Recommendation #7: Authorization for automated disclosure
Please find a link for Recommendation #7 here:
https://docs.google.com/document/d/11BSAUq1UOWJmZOSTaQIW0QZncnywljKJPWUtCTtnCHY/edit.

19. Choose your level of support of Recommendation #7:

Mark only one oval.

- Support Recommendation as written
- Support Recommendation intent with wording change
- **Significant change required: changing intent and wording**
- Recommendation should be deleted
- No opinion

20. If your response requires an edit or deletion of Recommendation #7, please indicate the revised wording and rationale here.

INTA feels strongly that day 1 automation should not be limited to law enforcement in EEA and dispute resolution provider requests. Instead, Disclosure should be fully automated from Day 1 for as many categories of request as is legally permissible. These categories should include as a minimum:

a. Requests from Law Enforcement in a jurisdiction local or applicable to the data subject;

b. Responses to UDRP and URS Providers for registrant information verification;

c. Requests where:
   i. the data subject is a legal person [to the extent that such information is not publicly available in whois]; and/or
   ii. neither the data subject nor the Contracted Party are subject to EU law [to the extent that such information is not publicly available in whois]; and/or
   iii. the data subject has consented to make their registration data public;

d. Requests that are made by officers of the court, made under penalty of perjury, and include a good faith assertion that a clearly identified and protectable intellectual property right is being infringed through use of an identified domain name, should also receive day 1 automation;

e. Requests relating to domains registered in new gTLDs that only permit legal entities to register domain names (e.g. .BANK).

“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” should be amended to read “Should the Central Gateway Manager determine that the request is incomplete, the Central Gateway Manager MUST reply with a response indicating that the request is incomplete, detailing which required data is missing, and providing an opportunity for the Requestor to amend its request “

“A Contracted Party MAY retract or revise a request for automation that is not required by these policy recommendations at any time.” Comment: There be some kind of notice period before this would go into effect, otherwise this could unduly prejudice requestors who are anticipating an automated process. The only exception should be if the Contracted Party must change its automation approach immediately by court order or in response to clear legal requirement that automation is not permitted in connection with the particular request or type of request.

Save Your Progress
21. Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time. 
Mark only one oval.

- Yes  Stop filling out this form.
- No, I wish to continue to the next section

Section 3, EPDP Phase 2 Recommendations #8-9

Recommendation #8: Response Requirements

Please find a link to Recommendation #8 here: https://docs.google.com/document/d/1U6iEnJzxls_824MsBzgW1tk7Qa2W6eY72B3QkdMu2Uk/edit?usp=sharing.

22. Choose your level of support of Recommendation #8:
Mark only one oval.

- Support recommendation as written
- Support intent of recommendation with edits
- Intent and wording of this recommendation requires amendment
- Delete recommendation
- No opinion

23. Do you recommend a change to the wording of Recommendation 8? If so, please indicate proposed edits and rationale here.

The timescale for sending out the confirmation should be expressed here. Only fully complete requests should be allowed to be submitted to allow for automation. Clarify whether the Requestor will have more than one opportunity to amend its request.

The requirement for the “Central Gateway Manager MUST immediately and synchronously respond with an acknowledgement response and relay the disclosure request to the responsible Contracted Party” conflicts with the “without undue delay” obligation in Recommendation 5. INTA prefers the obligation for an immediate acknowledgement response and relay (within 24 hours).

“and relay the disclosure request to the responsible Contracted Party”... How is this determined? Is it sent to the registrar or registry? Both? At the option of the requestor?

“As part of its relay to the responsible Contracted Party, the Central Gateway Manager MAY provide a recommendation to the Contracted Party whether to disclose or not. The Contracted Party MAY follow this recommendation.” How and when would this be determined? On what basis? Inconsistent Central Gateway Manager guidance could be viewed as prejudicing/advantaging certain parties which could be problematic for the system as a whole.

The disclosure response time should be more specific. In the absence of exceptional circumstances, the timeframe should be a maximum of 72 hours.
Responses should also identify how to appeal a determination or re-submit a request to address or overcome the reasons for denial. The EPDP should also consider the possibility of a lightweight, rapid, third-party dispute resolution system for challenging disclosure denials.

The phrase “imminent threat to life, serious bodily injury, critical infrastructure …” is explicitly intended to extend beyond EEA, but is so broad that it will likely result in disputes between requestors and contracted parties over what should qualify. INTA recommends the EPDP should develop an illustrative list, including for example, child exploitation, human trafficking, terrorism, etc. Apart from a penalty for requestors deemed to have abused Urgent SSAD Requests, there does not appear to be any mechanism to either help clarify this language or address inevitable disputes. Despite the ability to file complaints with ICANN, ICANN contractual compliance department will not insert itself as the arbiter to decide such disputes absent clear guidance on what qualifies and what does not qualify.

Rephrase to "Should the Central Gateway Manager establish that the request is incomplete, Central Gateway Manager MUST reply to the Requestor with a response indicating that the request is incomplete and detailing which data required by policy is missing, providing an opportunity for the Requestor to amend its request".

The timescale for sending out the confirmation should be expressed here. Clarify whether the Requestor will have more than one opportunity to amend its request.

The acknowledgement response MUST include a "ticket number" or unique identifier to allow for future interactions with the SSAD.

“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 requested by whom? The requestor? Compliance? Anyone?

“ICANN Compliance should be prepared to investigate complaints regarding disclosure requests under its enforcement processes.” What criteria will be used to evaluate these?

**Recommendation #9: Determining Variable SLAs for response times for SSAD**

Please find a link to Recommendation #9 here: [https://docs.google.com/document/d/1QwHyvi1SnFgVi8WGIlheCu0-fG76l_SIUFBe-sph-Ew/edit](https://docs.google.com/document/d/1QwHyvi1SnFgVi8WGIlheCu0-fG76l_SIUFBe-sph-Ew/edit).

24. Choose your level of support of Recommendation #9:
   - Mark only one oval.
   - Support recommendation as written
   - Support intent of recommendation with edits
   - **Intent and wording of this recommendation requires amendment**
   - Delete recommendation
   - No opinion

25. Do you recommend a change to Recommendation 9? If so, please indicate proposed edits and rationale here.

   All Priority 2 cases should be capable of automation from Day 1.
The Contracted Party should receive the disclosure request from the Central Gateway Manager on the same day that it was filed (as per Recommendation 8.b)

If the Mechanism for the evolution of SSAD identifies additional categories of requests that could be fully automated, the SSAD MUST allow for automation of their processing and the requests MUST be automatically processed and result in the disclosure of non-public RDS data without human intervention if legally permissible.

“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 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.” Where a UDRP or URS filing is contemplated/imminent this should be sufficient to retain priority 2 status even if the complaint has not yet been filed.

26. If you do not agree with the proposed SLA matrix and/or accompanying description, please provide your rationale and proposed alternative language.

INTA understands it will take some time for contracted parties to come into compliance with any SLA’s that are selected. However, INTA favors a uniform SLA for all priority 3 requests plus a simple contractual compliance grace period over the proposed bifurcated phases, mean response time measurements, and compliance percentage proposals. INTA also strongly supports a maximum 3 business day SLA for Priority 3 requests. Specifically, INTA further recommends that:

a. the suggested 3 business day SLA apply to all priority 3 requests, with a six-month contractual compliance grace period for contracted parties to meet this SLA. To the extent that there are different SLAs for priority 3 requests based on phases, it does not make sense that the SLAs would be shorter during the first phase while the contracted party is trying to implement the SLAs and then longer after the contracted party has had more time to implement the system.

a. The use of a mean response time and compliance percentage proposals make it impossible for ICANN or the community to hold any individual contracted party accountable for noncompliance.

b. Likewise, they make it difficult for any individual contracted party to know whether it has complied with the SLA’s in real-time. Under the proposed process, the contracted party is only able to determine whether it has complied with the SLAs after the fact.

ICANN should provide economic incentives for contracted parties with faster mean response times.

“These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention if legally permissible.” How will legal permissibility be determined? Any requests that can be legally automatically processed and result in disclosure of non-public RDS data MUST be. It should not be discretionary or allow for variance between different Contracted Parties. If certain Contracted Parties are automatically granting disclosure for certain types of requests, all other Contracted Parties should be granting disclosure for similarly situated requests either in an automated manner or, if due to resources automation is not possible for a particular Contracted Party, they must still be manually disclosed but with the same disclosure outcome unless there is a legal reason for not doing so (e.g. under local law of the CP).
27. Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.

Mark only one oval.

☐ Yes  Stop filling out this form.

☐ No, I wish to continue to the next section

Section 3, EPDP Phase 2 Recommendations #10-16

Recommendation #10: Acceptable Use Policy

Please find a link to Recommendation #10 here:
https://docs.google.com/document/d/1JHgbtfvnHezDhEJLkJ6KxyGC1byGu1v7XZA73Z47IMA/edit?usp=sharing. Choose your level of support of Recommendation #10:

Mark only one oval.

☐ Support recommendation as written

☐ Support intent of recommendation with edits

☐ Intent and wording of this recommendation requires amendment

☐ Delete recommendation

☐ No opinion

28. If your response requires an edit or deletion of Recommendation #10, please indicate the revised wording and rationale here.

(a) “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.” According to whom? The CGM? A third-party? This could be clarified regarding who can trigger enforcement mechanism regarding “apparent misuse.”

(b) Limiting requested data to only the current RDS will impose a challenge on brand owners and other third-party requestors. In addition to learning the identity of a current domain name registrant, it is very important for a brand owner to learn the approximate date on which that registrant acquired the disputed domain (sometimes through purchase from a prior registrant and thus, different from the domain’s creation date). This is because both the UDRP and URS require a showing of bad faith registration and use, i.e., bad faith at the time the disputed domain name was acquired by the registrant. By limiting requested and disclosed data only to the current information, brand owners may not be able to ascertain whether the registrant’s acquisition of the disputed domain name predates the brand owner’s trademark rights. This could result in the unintended filing of UDRP or URS complaints that have no chance of success. In such instances brand owners, through no fault of their own, could be found guilty of reverse domain name hijacking. In order to avoid this risk, requested data should not be limited to current RDS but should, upon request, be expanded to include archived/historical data as well to the extent such data is available.

(c) The “representations” required by this Recommendation must not be unduly burdensome and should, ideally, be satisfied by a check-the-box list of common reasons for such requests (with a catch-all “Other” checkbox and free text field for stating uncommon reasons). As for the “corresponding purpose and lawful basis for the processing”, the
comments set forth pertaining to Preliminary Recommendation #3 “Criteria and Content of Requests” are incorporated here as well.

(d) No comment.

(e) It is unclear what is meant by the “representation regarding the intended use of the requested data”. If this simply means that the requestor represents that the intended use is valid, then this should be satisfied by a simple checkbox. However, if it’s meaning is intended to be broader and mean that the intended use must be specifically stated, this seems to be redundant to other parts of the process set out in the recommendations. If the latter is the case, then the representation should be satisfied by a standardized check-the-box list of common intended uses (with a catch-all “Other” checkbox and free text field for stating uncommon uses). Further, the “representation that the requestor will only process the data for the stated purpose(s)” should be satisfied with a simple checkbox.

(f) No comment.

**Recommendation #11: Disclosure Requirement**

Please find a link to Recommendation #11 here: [https://docs.google.com/document/d/1r6qgmnl-0ha0mmYqP0Z3drZr3FJxsG-uW9bRC2bJ4Uo/edit?usp=sharing](https://docs.google.com/document/d/1r6qgmnl-0ha0mmYqP0Z3drZr3FJxsG-uW9bRC2bJ4Uo/edit?usp=sharing).

29. Choose your level of support of Recommendation #11:

   Mark only one oval.

   - Support recommendation as written
   - Support intent of recommendation with edits
   - **Intent and wording of this recommendation requires amendment**
   - Delete recommendation
   - No opinion

30. If your response requires an edit or deletion of Recommendation #11, please indicate the revised wording and rationale here.

   As an initial matter, same comment as above regarding who/how mechanism is triggered regarding “apparent misuse.”

(a) No comment.

(b) Prohibiting historic data and limiting requested data to only the “current data or a subset thereof” will impose a challenge on brand owners See comments pertaining to Recommendation 10 a), which are applicable here as well.

(c) The term “applicable law” should be defined as it is confusing and unduly broad in relation to a contractually-based, multi-national system such as the DNS. Does “applicable law” mean that which is applicable in the jurisdiction of the requestor, the Identity Provider, the registrant, the registrar, the registry, or of ICANN? Or does it mean all of the various laws of all of these jurisdictions?

(d) While there is no objection to logging requests, further details should be specified such as where such logs are to be maintained, by whom, and for how long.

(e) With respect to the “balancing test”, the comments pertaining to the balancing test set out in Recommendation #6, par. 5 are incorporated here as well.
(f) The term “reasonable request” should be defined so as to avoid any improper denials of requested data and any unnecessary delays in processing the same. Should also clarify that the request is by the data subject.

(g) The term “applicable law” should be defined. The comments pertaining to Recommendation 11 par. (c) above are incorporated here as well. Further, while providing a “mechanism under which the data subject may exercise its right to erasure and any other applicable rights” is quite reasonable in principle, care must be taken that this is presented in a neutral manner such that the data subject is neither encouraged to, nor discouraged from exercising any such rights. Nevertheless, any such erasure should be done only after the requested information is provided to the requestor. The right to erasure cannot serve as a mechanism for a cybersquatter or criminal to evade the consequences of its actions.

(h) The “privacy policy for the SSAD and standard language (relating to the SSAD) to inform data subjects” should be developed by the SSAD stakeholders and put out for public comment to ensure the clarity, accuracy, and neutrality of the same. Further, the comments pertaining to Preliminary Recommendation #4 Third Party Purposes / Justifications are incorporated here as well.

(i) It is important that “the nature of legal investigations or procedures” not be limited to criminal investigations by law enforcement or other governmental entities. There are situations where civil investigations may require that requests be kept confidential from the data subject (e.g., where counterfeit goods may be quickly sold or destroyed by a data subject in an attempt at frustrating the enforcement of intellectual property rights). Further, the term “applicable law” should be defined and the comments to Recommendation 11 par. c) above are incorporated here as well.

Recommendation #12: Query Policy

Please find a link to Recommendation #12 here: https://docs.google.com/document/d/1_ng86GC09Ye5ruCBk4vBrXZN7nCyagAanJT9aSDBrGQ/edit?usp=sharing.

31. Choose your level of support of Recommendation #12:

   Mark only one oval.

   ○ Support recommendation as written
   ○ Support intent of recommendation with edits
   ◯ Intent and wording of this recommendation requires amendment
   ○ Delete recommendation
   ○ No opinion

32. If your response requires an edit or deletion of Recommendation #12, please indicate the revised wording and rationale here.

   (a) In defining “abuse or misuse of the system” the comments pertaining to Preliminary Recommendation #1: Accreditation, pars. o) – s) (Accredited User Revocation & Abuse), par. t) (De-authorization of Identity Providers), and to Preliminary Recommendation #8. Response Requirements, par. d) (Abuse of urgent requests) are incorporated here as well.

   (b) 1. and 2. The term “High volume” should be defined. Further, although “redress via ICANN” is provided for, it is likely to be slow even in the face of an urgent need for the disclosure of information. Something faster is needed. Reasonable exceptions should be
allowed for innocent errors that are neither intentionally malformed/incomplete or frivolous/vexatious. For example, there may be instances where a legitimate requestor submits a single, batched series of requests (e.g., where the same registrant owns a large number of disputed domain names) that are malformed or incomplete due to a minor and unintentional human error. In such situations, the requestor should be given notice of the deficiency(ies) by the entity receiving requests and then permitted an expedited (i.e., 24-hours or less) opportunity to cure them and resubmit the requests. Further, ICANN org as used in this section should be more specific – should it refer to ICANN Compliance or some other structure within ICANN org?

(c) In addition to “specific domain name[s]”, provision should be made for disclosure, upon request, of all domain names owned by the same registrant who is the owner of the specific domain name that is the subject of the initial request. In UDRP and URS cases one of the stated methods of proving bad faith is to submit evidence of a registrant’s “pattern of conduct” involving the registration of other domain names that are confusingly similar to either the complainant’s or to a third-party brand owner’s trademarks. As such, this can be a critical piece of evidence in a UDRP or URS case. However, in light of widespread masking of registrant information, even with respect to registrants for whom GDPR does not apply, finding evidence of a pattern of conduct through common domain name ownership has become almost impossible. This information is only within the possession of the registrar and registry (or it might be spread across different registrars and registries used by the registrant) and so should be available to accredited Requestors for legitimate and lawful purposes such as protecting the public from harm and protecting the integrity of intellectual property rights. In addition, EPDP should consider introducing some kind of “trusted requestor” program to expedite responses to similarly-situated requests from a trusted requestor based on pre-defined criteria and use cases.

With respect to the statement, in Recommendation 12, that “historical registration data will not be made available via this mechanism”, prohibiting historic data will impose a challenge on brand owners. As such, the comments pertaining to Recommendation 10 a) are incorporated here as well.

**Recommendation #13: Terms of Use**

Please find a link to Recommendation #13 here: [https://docs.google.com/document/d/1ou3hY3peDnxgo45FmUBs_clv4f3qUntYeclq10wB_4/edit?usp=sharing](https://docs.google.com/document/d/1ou3hY3peDnxgo45FmUBs_clv4f3qUntYeclq10wB_4/edit?usp=sharing).

33. Choose your level of support of Recommendation #13:

*Mark only one oval.*

- [ ] Support recommendation as written
- [X] Support intent of recommendation with edits
- [ ] Intent and wording of this recommendation requires amendment
- [ ] Delete recommendation
- [ ] No opinion

34. If you believe edits are needed for Recommendation #13, please propose edits and rationale here.

INTA supports the concept of using appropriate agreements, such as terms of use, a privacy
policy and a disclosure agreement to provide rights, duties and obligations concerning access and disclosure of data through SSAD. However, such agreements must be carefully drafted and vetted by the community so that they accurately reflect EPDP policy recommendations and not impose additional obligations or duties or provide imprecise access or disclosure rights. All SSAD stakeholders should be involved in developing these agreements. The EPDP should also clarify how a code of conduct would relate to terms of use and the other agreements discussed in this recommendation, and consider whether all of these agreements could be covered under a single terms of use document.

INTA recommends the following revisions to Recommendation #13:

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 accurately reflect the recommendations of the final reports of the EPDP Team. These agreements are expected to be developed and negotiated by all SSAD stakeholders, taking the below implementation guidance into account and any such draft agreements will be published for public comment prior to implementation.

With respect to recommendations concerning proposed Terms of Use, INTA believes that a standard of mere misrepresentation to trigger requestor indemnification should be revised to an “intentional, reckless or willful” behavior standard. Misrepresentation is ultimately a vague legal principal without further qualification, such as fraudulent, negligent or innocent, to provided context. Moreover, misrepresentation can include merely misleading statements, including unintentional ones.

“The EPDP recommends, at a minimum, the privacy policy SHALL include:
● Relevant data protection principles, for example,”. Were there supposed to be particular examples listed here?

“Applicable prohibitions Disclosure” Should this say “Applicable prohibitions on Disclosure”?
Please clarify

**Recommendation #14: Retention and Destruction of Data**

Please find a link to Recommendation #14 here: https://docs.google.com/document/d/1tBf2jEWtYydskYMgXxYAjOObGboFgL4IYJHq9b9wdo86pU/edit?usp=sharing.

35. Choose your level of support of Recommendation #14:
Mark only one oval.

- Support recommendation as written
- Support intent of recommendation with edits
- Intent and wording of this recommendation requires amendment
- Delete recommendation
- No opinion

36. If you do not support Recommendation #14, please provide proposed edits and rationale here.

With respect to Recommendation #14, INTA supports the recommendation “that requestors MUST confirm that they will store, protect and dispose of the gTLD registration data in
accordance with applicable law.”

However, the second sentence of Recommendation #14 will create a contradiction if the registration data itself must be retained by applicable law:

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

This second sentence appears to be inspired by the GDPR. However, GDPR does not specify retention periods for personal data, which will often be supplied by “applicable law”. Instead, it states that personal data may only be kept in a form that permits identification of the individual for no longer than is necessary for the purposes for which it was processed. This provision of the GDPR is subject to debate and various interpretations when there is a legal right or obligation to keep the personal data. This balancing concept of reasonableness is not (and cannot realistically) be part of Recommendation #14. As such, the last sentence of Recommendation #14 is not needed and could create two conflicting obligations for Requestors. For instance, an investigator may need to keep evidence until a statute of limitations has run, but the purpose of the investigation may end after an arrest is made. The second sentence of Recommendation #14 should be struck.

Recommendation #15: Financial Sustainability

Please find a link to Recommendation #15 here: https://docs.google.com/document/d/1EN7mDz44BkxoW_RVlDsgjhxSLkUgrW5XwIx-O-0TEk/edit?usp=sharing.

37. Choose your level of support of Recommendation #15:
   Mark only one oval.
   - Support recommendation as written
   - Support intent of recommendation with edits
   - Intent and wording of this recommendation requires amendment
   - Delete recommendation
   - No opinion

38. If you believe edits are needed for Recommendation #15, please propose edits and rationale here.

INTA agrees that there needs to be a delineation in costs between the development of the SSAD system and its operational costs. INTA further agrees that development costs should be initially borne by ICANN org, and Contracted Parties.

INTA further agrees that the subsequent running of the system should be on a cost recovery basis and that historic costs may be considered. In developing fees for access and accreditation for cost recovery, INTA asserts that fees for one class of user or accreditation applicant cannot be charged that are so high as to circumvent the policies developed by the EPDP Team. For instance, a corporate entity should not be charged a fee that makes access or accreditation an impracticable or expensive undertaking simply because they have large number of trademarks or a greater need for using the SSAD for enforcement purposes. INTA asserts that financial burden on all parties to the system should be equal or at least proportionate.

We would also support allocation of ICANN budget toward offsetting the costs for maintaining the Central Gateway and in general for setting up and maintaining this system.

We would like further specifics regarding the suggested legal risk fund and why such a fund is
necessary as part of the costs of this system. All businesses and systems operate subject to some legal risk, so it is not clear why this system necessitates a special fund for its risks.

Finally, this section refers to “input from ICANN Org concerning the expected costs of developing, operationalizing and maintaining the three different models.” Can EPDP clarify what it means by “three different models” as used here?

**Recommendation #16: Automation**

Please find a link to Recommendation #16 here: [https://docs.google.com/document/d/1_gqq1JKHcDqVKKfwdwOdfAghPYm-ErV2t9qxJVDsDjWc/edit?usp=sharing](https://docs.google.com/document/d/1_gqq1JKHcDqVKKfwdwOdfAghPYm-ErV2t9qxJVDsDjWc/edit?usp=sharing).

39. **Choose your level of support of Recommendation #16:**

   *Mark only one oval.*

   - Support recommendation as written
   - Support intent of recommendation with edits
   - **Intent and wording of this recommendation requires amendment**
   - Delete recommendation
   - No opinion

40. **If you believe changes are needed for Recommendation #16, please provide proposed edits and rationale here.**

   - Automation of the receipt, authentication, and transmission of System for Standardized Access/Disclosure (“SSAD”) requests as well as automated disclosure of non-public registration data is an important and positive mechanism that will allow more efficient response to DNS abuse. However, the proposed recommendations severely limit the types of disclosure requests to be fully automated on Day 1, such that the potential benefit of automation is denied to many accredited users with legitimate types of disclosure requests.

   - **See Preliminary Recommendation #7. Authorization for automated disclosure requests,** “The EPDP Team expects that the following types of disclosure requests can be fully automated (in-take as well as response) from the start:

     - Requests from Law Enforcement in local or otherwise applicable jurisdictions;
     - Responses to UDRP and URS Providers for registrant information verification.

   - As stated above in the response to Recommendation #7, INTA feels strongly that Day 1 automation should not be limited to law enforcement in EEA and dispute resolution provider requests. Instead, disclosure should be fully automated Day 1 for as many categories of request as is legally permissible.

   - Importantly, brand owners’ requests are absent from the EPDP Team’s limited types of automated disclosure requests. INTA feels strongly that this must be revised to include requests by brand owners that go through the accreditation process, outlined in Preliminary Recommendation #1. In the case of an accredited brand owner that requests disclosure of non-public registration data behind a domain where the Requestor has presented a well-founded allegation of infringement of the brand owner’s established intellectual property rights as the purpose for the disclosure request, there is no reason that automation would not be feasible or legally permissible. Accordingly, it is important that the EPDP Team
Save Your Progress

41. Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.
Mark only one oval.

☐ Yes Stop filling out this form.
☐ No, I wish to continue to the next section

Section 3, EPDP Phase 2 Recommendation #17

Recommendation #17: Logging

Please find a link to Recommendation #17 here: https://docs.google.com/document/d/1zG2myy1br-xbXBHvd34gm_J-vXPER6GoOoWFq9RQ/edit?usp=sharing.

42. Choose your level of support of Recommendation #17:
Mark only one oval.

☐ Support recommendation as written
☐ Support intent of recommendation with edits
☐ Intent and wording of this recommendation requires amendment
☐ Delete recommendation
☐ No opinion

43. If you believe changes are needed for Recommendation #17, please provide proposed edits and rationale here.

INTA supports the above logging requirements of requests and responses as such logging serves the important purpose of allowing ICANN Compliance to audit the actions of disclosing entities, identifying any instances of systemic non-compliance, and take appropriate enforcement action. Audits will, among other things, ensure the SSAD system is functioning properly, and is not being abused by accredited individuals or entities that materially breached the conditions of accreditation. Additionally, accredited users who are in compliance will have the benefit of the backstop provided by the logging and audit systems, if ever a user needs to challenge a denial of a data disclosure request.

Section 3, EPDP Phase 2 Recommendations #18-19, Implementation Guidance

Recommendation #18: Audits
44. Choose your level of support of Recommendation #18:

Mark only one oval.

☐ Support recommendation as written
☐ Support intent of recommendation with edits
☐ Intent and wording of this recommendation requires amendment
☐ Delete recommendation
☐ No opinion

45. If you do not support Recommendation #18, please provide proposed edits/changes and rationale here.

INTA supports the SSAD having robust audit mechanisms to enable monitoring and compliance with law and with ICANN policy. While INTA notes that Recommendation 18 “expects” that auditing is done to ensure compliance, we note that this expectation in its current form does not use the term “recommend,” nor does it explicitly recommend auditing contracted parties. INTA assumes this to be a drafting oversight, but in the interest of clarity, INTA submits that Recommendation 18 should contain an explicit policy recommendation to audit contracted parties’ compliance with this policy.

We also note that the recommendation states “ICANN org as the Accreditation Authority is not required to audit governmental entities, whose accreditation and audit requirements are defined in Preliminary Recommendation #2.” If ICANN org is not the Accreditation Authority, would a third-party Accreditation Authority be required to audit governmental entities, or would any Accreditation Authority be exempt from auditing governmental entities? What is the rationale for this and for any distinction in auditing requirements as between ICANN org versus a third-party Accreditation Authority when it comes to auditing governmental entities?

This section also states “As 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.” We assume this should say “IF ICANN serves as....”

Recommendation #19: Mechanism for the Evolution of the SSAD

Please find a link to Recommendation #19 here:
https://docs.google.com/document/d/12KdBUNUXy8m_exDvFL3D2rBUYUTMmJpM9RgoWiZL_0o/edit?usp=sharing

46. Choose your level of support of Recommendation #19:

Mark only one oval.

☐ Support recommendation as written
☐ Support intent of recommendation with edits
☐ Intent and wording of this recommendation requires amendment
☐ Delete recommendation
☐ No opinion
47. If you do not support Recommendation #19, please provide proposed edits or changes and rationale here.

As a threshold matter, INTA questions the necessity of such a Mechanism. INTA notes that the EPDP team decided to deviate from its longstanding preference for a centralized model only as a result of a misinterpretation of a letter received from the Belgian DPA (https://www.icann.org/en/system/files/correspondence/stevens-to-marby-04dec19-en.pdf). With the record corrected that the Belgian DPA actually thinks that a centralized model is a “better, ‘common sense’ option in terms of security and for data subjects”, INTA submits that the EPDP should complete its work based on such a centralized model. (https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority)

Should the EPDP team decide that such a Mechanism remains necessary, the composition of the Mechanism must represent the entire ICANN community, and not merely those interests represented in the GNSO. It is critical that such a Mechanism reflects the needs and interests of SSAD users including governments, cybersecurity investigators, and internet users at large.

If such a Mechanism is developed, it should be chartered with the power and scope to operate in one clear direction: to move as swiftly as possible toward the greatest amount of standardization (by centralization) and automation as legally possible. The Mechanism must not be allowed to undo any requirements for standardization, centralization, or automation developed by the EPDP team without citing clear, unambiguous legal risk associated with the status quo. With this sole exception, its only goal should be to add use cases which can be standardized, centralized, and automated based on new legal clarity. If this Mechanism is intended to act as a future corrective measure addressing the current lack of legal clarity, it must simultaneously have the power to require new request types to be automated without that power being deemed policymaking such that it fall under the exclusive control of the GNSO. INTA urges that great caution must be taken to achieve this end, and INTA reiterates that the difficulty presented here further supports that developing a centralized model at the outset remains preferable.

If it is ultimately determined that the Mechanism is needed, we might look to other forms of standing committees employed by ICANN to continuously examine and recommend improvements to other matters, e.g. the IANA Customer Standing Committee, the Empowered Community structure, the GNSO Council Standing Selection Committee, etc. Representation within this Mechanism should reflect the representative makeup of the EPDP itself (including GNSO stakeholders as well as ALAC, SSAC, and GAC) and its guidance could be channeled to the GNSO Council, ICANN Org, and Board, with implementation of any accepted evolutionary guidance handled by a “standing” ICANN Org IRT in coordination with the standing committee Mechanism.
48. What existing processes / procedures, if any, can be used to meet the above responsibilities?


49. If no suitable existing processes / procedures can be used, what type of mechanism should be created factoring in: Who should guidance be provided to? How is guidance developed / agreed to? How should it be structured?


50. What information is needed to ensure the continuous evolution of SSAD?


51. How is guidance of the Mechanism expected to be implemented?


**Implementation Guidance #i.**

Please find a link to Implementation Guidance #i. here: [https://docs.google.com/document/d/1uh3VfWkOZyU7NpVupPU7VBuoW6Lo1N65HUUPnGbBgr4/edit?usp=sharing](https://docs.google.com/document/d/1uh3VfWkOZyU7NpVupPU7VBuoW6Lo1N65HUUPnGbBgr4/edit?usp=sharing).
52. Choose your level of support of Implementation Guidance #i:
Mark only one oval.

- Support implementation guidance as written
- Support implementation guidance with edits
- Intent and wording of this implementation guidance requires amendment
- Delete implementation guidance
- No opinion

53. If you do not support Implementation Guidance #i, please provide proposed edits or changes and rationale here.

---

**Reporting Requirements**

Implementation Guidance #ii currently provides: Following the public comment period, the EPDP Team will further review what reporting requirements are necessary to support the SSAD.

54. What type of reporting should be required as part of SSAD?

INTA strongly supports robust reporting on all measurable aspects of SSAD, with requirements that all registries and registrars, Accreditation Authorities and Identity Providers, and ICANN (and any other parties that may facilitate any aspect of SSAD) maintain metrics data concerning the aspects of the system for which they are responsible, and that ICANN should be required to regularly publish compilations of such data. The types of metrics that should be reported might include total numbers of accredited parties, number of accreditation requests that were denied, total number of disclosure requests made through SSAD, total number of disclosure requests acknowledged within SLA timeframe and total number not timely acknowledged, total number of disclosure requests granted and denied and how many were substantively responded to within SLA timeframe versus beyond this timeframe, and the breakdown of legal bases and purposes for all disclosure requests (both granted and denied). It would also be helpful to make such data available on a per-registry and per-registrar basis. We would be happy to provide further input on a specific reporting program proposal, which should be developed as part of SSAD implementation.

**Other Comments & Submission**

55. Are there any recommendations the EPDP Team has not considered? If yes, please provide details below.

At a high level, the EPDP should revisit the possibility of a centralized SSAD model, in light of apparently inconsistent comments on this subject, calling into question whether such an approach would actually be impermissible under GDPR. INTA would strongly prefer a more centralized/automated approach to SSAD that is more reflective of the historical WHOIS system in terms of querying and disclosure of data.

In any event, the EPDP must present a recommendation for a mechanism for obtaining historical data, to the extent such data is retained by Contracted Parties/ICANN. The EPDP must also present a recommendation for a mechanism for conducting “reverse RDDS” searches to identify all domain names.
associated with a particular RDS data element (e.g. name or email address). These functions are critical components for many third-party end-users of SSAD, including law enforcement, cybersecurity, consumer protection and intellectual property owners/agents. The EPDP should also specifically recommend automatic disclosure of any data that is not subject to GDPR, including data of legal persons and where the data is otherwise not subject to GDPR on jurisdictional grounds (i.e. no party in the data flow is subject to EU law, including registrant and registrar/registry)

56. Are there any other comments or issues you would like to raise pertaining to the Initial Report? If yes, please enter your comments here. If applicable, please specify the section or page number in the Initial Report to which your comments refer.