ICANN | GNSO

Generic Names Supporting Organization

Standard System for Access/Disclosure (SSAD) Supplemental Recommendations

BACKGROUND **2**
INTRODUCTION TO SUPPLEMENTAL RECOMMENDATIONS "CHAPEAU" **2**
UPDATED RECOMMENDATION ORDER **2**
SUPPLEMENTAL RECOMMENDATIONS **2**
- Glossary 3
- Supplemental Recommendation 1: Authentication 4
- Supplemental Recommendation 2 [3]: Criteria and Content of Requests 10
- Supplemental Recommendation 3 [4]: Acknowledgement of Receipt and Relay of the Disclosure Request 13
- Supplemental Recommendation 4 [6]: Request Types and Service Level Agreements 15
- Supplemental Recommendation 5 [8]: Contracted Party Disclosure Decision 19
- Supplemental Recommendation 6 [11]: SSAD Agreements and Policies 22
- Supplemental Recommendation 7 [13]: Query Abuse Policy 26
- Supplemental Recommendation 8 [14]: Financial Sustainability 29
- Supplemental Recommendation 9 [15]: Logging 31
- Supplemental Recommendation 10 [16]: Auditing 33
- Supplemental Recommendation 11 [17]: Reporting 35
- Supplemental Recommendation 12 [18]: SSAD Standing Committee 36

High-Level Summary of Impact Assessment **39**
Annex 1 – Original Working Draft Recommendation Order **40**
Annex 2 – SSAD Supplemental Recommendations Team Assignment Form **42**

BACKGROUND

On 12 March 2026, the ICANN Board resolved not to adopt the 18 pending SSAD recommendations from the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process. As indicated in the ICANN Bylaws[1], the GNSO Council, "shall meet to affirm or modify its recommendation, and communicate that conclusion (the "Supplemental Recommendation") to the Board, including an explanation for the then-current recommendation."

Herein contained are the GNSO Council's Supplemental Recommendations related to recommendations not adopted by the ICANN Board.

INTRODUCTION TO SUPPLEMENTAL RECOMMENDATIONS "CHAPEAU"

The GNSO Council is providing Supplemental Recommendations for a centralized system to facilitate the disclosure of nonpublic registration data. These Supplemental Recommendations establish policy requirements and expected system capabilities but are not intended to prescribe or presuppose a particular technical or operational implementation. The SRT intends for the Supplemental Recommendations to provide ICANN org with sufficient flexibility to determine how best to implement the required functionality, consistent with the policy requirements set forth in the Supplemental Recommendations.

Accordingly, the Supplemental Recommendations are intended to be implementation and technology agnostic. For example, ICANN org may determine that the Supplemental Recommendations can be implemented through enhancements to the existing Registration Data Request Service (RDRS), through the procurement of services from a third-party provider, or through another implementation approach that satisfies the requirements of these Supplemental Recommendations.

UPDATED RECOMMENDATION ORDER

The SSAD Supplemental Recommendations Team ("SRT"), or the team tasked by the GNSO Council to develop Supplemental Recommendations, reviewed the original 18 SSAD recommendations and ultimately produced 12 Supplemental Recommendations for the GNSO Council's consideration. The updated number of recommendations is the result of consolidating text and removing text the SRT found no longer fit for purpose. A detailed comparison of the original numbering and new numbering can be found in Annex 1 – Original Working Draft Recommendation Order.

SUPPLEMENTAL RECOMMENDATIONS

In reviewing these Supplemental Recommendations and associated Implementation Guidance, the SRT notes the following terminology.

[1] See ICANN Bylaws, Annex A, Section 9.

Supplemental Recommendation: The SRT expects that the GNSO Council and ultimately the ICANN Board will approve and implement all provided Supplemental Recommendations, and ICANN org will work closely with an Implementation Review Team (IRT) to ensure that implementation takes place in line with the SRT's intent. The Supplemental Recommendations often address what the SRT recommends takes place, as opposed to how it should take place. The Supplemental Recommendations typically use the term "MUST," indicating that the recommended action is required to take place and/or necessary.

Implementation Guidance: The SRT strongly recommends the stated action, with a strong presumption that it will be implemented, but recognizes that there may exist valid reasons in particular circumstances to not take the recommended action exactly as described. However, the party to whom the action is directed must make all efforts to achieve the purpose behind the recommended action (as expressed in the rationale and the recommendation to which the implementation guidance is linked, if applicable) even if done through a different course. In all cases, the full implications must be understood and carefully weighed before choosing a different course. Implementation guidance commonly refers to how a recommendation should be implemented.

Glossary

Term	Definition
Authenticated Requestor	A person acting on behalf of an organization, or an individual, who meets the requirements applicable to a Standard Requestor and whose identity and organizational affiliation have been verified by an Authentication Provider in accordance with ICANN's published administrative, technical, and security requirements. Authenticated status provides assurance of identity/affiliation only and does not create any entitlement to disclosure.
Authentication	A process of verifying the requestor's organizational affiliation, and where applicable, the identity of a requestor, and issuing an Authentication Token that may be relied upon by Contracted Parties. In the SSAD example, authentication could mean a process used to establish that a requestor represents a law enforcement agency.
Authentication Provider	An entity who has been recognized by ICANN org or its designee(s) as having met the policy requirements for qualified Authentication Providers as outlined in the ICANN policy and supporting documents.

Term	Definition
Authentication Token	A cryptographically verifiable statement issued by an Authentication Provider regarding the authenticated status of the requestor. The term "Authentication Token" is technology- and protocol-neutral and is not intended to prescribe or require the use of any particular authentication protocol, standard, or token format. For the avoidance of doubt, the term "Authentication Token" is used generically and does not prescribe any particular authentication protocol, standard, or technical implementation (e.g., OpenID Connect, SAML, or successor technologies).
Authorization	The act of granting a party permission to do something. In the SSAD example, a Contracted Party may authorize the disclosure of requested data elements to a requestor.
Critical Infrastructure	Critical infrastructure means the physical and cyber systems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety.
Personal Data	Any information relating to an identified or identifiable natural person (a "Data Subject").
Standard Requestor	A person acting on behalf of an organization, or an individual who (i) has an SSAD account, which at a minimum, requires a verified email address; and (ii) submits to the SSAD Agreements and Policies.[2] Having met the requirements in (i) and (ii), this requestor may submit disclosure requests for non-public registration data through the SSAD.

Supplemental Recommendation 1: Authentication

Supplemental Recommendation 1 was also numbered as Recommendation 1 in the original EPDP Phase 2 SSAD recommendations; however, Supplemental Recommendation 1 also includes text from the original SSAD Recommendation 2.

Requestor Categories

[2] Please see Supplemental Recommendation 6 for details on the SSAD Agreements and Policies.

1.1. The SSAD MUST support two categories of requestors: Standard Requestors and Authenticated Requestors.

1.2. All requestors MUST establish an SSAD account in accordance with the requirements established for use of the system.[3]

Authentication Providers

1.3. ICANN org or its designee, in consultation with the Implementation Review Team (IRT) during implementation, MUST establish, publish, and maintain a framework, which includes the administrative, technical, and security requirements under which organizations may become recognized Authentication Providers. The framework MUST include an appropriate mechanism to bind recognized Authentication Providers to compliance with applicable framework requirements. Following implementation, ICANN org or its designee SHOULD consult the Standing Committee on proposed changes to the framework. The following elements SHOULD be included in the requirements published by ICANN org for the recognition of Authentication Providers, but additional elements MAY be included.

1.3.1. Minimum requirements for determining the eligibility requirements of Authenticated Requestors, taking into account the community or category of Requestors served by the Authentication Provider.

1.3.2. Minimum requirements for Authentication procedure

1.3.3. Minimum requirements for Authentication credential management policies, e.g., lifetime, expiration, renewal frequency, security properties (password or key policies/strength), etc.

1.3.4. Minimum requirements for Authentication credential revocation procedures: circumstances for revocation, including, for example, what constitutes abusive use of credentials, revocation mechanism(s), etc.

1.3.5. Minimum requirements for Authentication Providers' auditing procedures of their Authenticated Requestors, including how Authenticated Requestors are audited and how frequently the auditing occurs.[4]

1.4. ICANN org or its designee MUST recognize Authentication Providers that satisfy the published requirements. ICANN org or its designee is responsible for managing the application and recognition process for Authentication Providers, including reviewing applications, and determining whether applicants satisfy the published requirements established in consultation pursuant to Section 1.3.

1.5. At a minimum, the SRT expects that an entity seeking to be an Authentication Provider will be responsible for the following:

---

[3] See Supplemental Recommendation 6: Agreements and Policies for additional information regarding the agreements and policies that a requestor is required to agree to in order to submit requests through the SSAD system.

[4] Please note this is distinct from the auditing of Authentication Providers, which is described in Supplemental Recommendation 10.

1.5.1. Verifying the identity and organizational affiliation of the applicant using reliable evidence or authoritative sources appropriate for the community it serves.

1.5.2. Verifying the applicant is authorized by its employer/affiliated organization to request registration data as an Authenticated Requestor (for example, approved to request registration data in the capacity of a law enforcement agent).

1.5.3. Protecting personal information obtained during identity verification/proofing.

1.5.4. Determining whether the applicant satisfies the Authentication Provider's documented authentication procedures.

1.5.5. Where user satisfies the Authentication Provider's documented procedures, establishing an authenticated account and issuing an authentication credential capable of generating an Authentication Token.

1.5.6. Maintaining an authoritative registry of its Authenticated Users.

1.5.7. Maintaining procedures for periodic review, suspension, renewal, and revocation of authenticated status, including the application of graduated penalties for violations and an appeal mechanism that permits an Authenticated Requestor to challenge suspension or revocation before it takes final effect.

1.5.8. Meeting the technical requirements established by ICANN org or its designee for integration with the SSAD.

1.5.9. Maintaining sufficient records to demonstrate that authentication activities have been performed in accordance with ICANN org or its designee's published administrative, technical, and security requirements in order to support audits and compliance reviews.

Note: The list provided in 1.5.1 - 1.5.9 MAY be further adjusted during implementation, in consultation with relevant stakeholders as appropriate, to provide flexibility, address changes in technology or security, etc. Relevant stakeholders means the IRT before the policy goes into effect and the Standing Committee, after the policy goes into effect.

Authentication Tokens

1.6. The SRT expects that the SSAD would facilitate the transmission of an Authentication Token from an Authenticated Requestor to a Contracted Party. The SRT expects that Authentication Providers will issue an Authentication Token to an Authenticated Requestor that enables a Contracted Party to validate authenticated status. For the avoidance of doubt, Authentication establishes identity and organizational affiliation only. Disclosure decisions remain the responsibility of the applicable Contracted Party as outlined in Supplemental Recommendation 5. Neither authentication nor authenticated status creates a presumption that non-public registration data will be disclosed.

1.7. The Authentication Token MUST securely transmit the minimum authentication attributes required to support the Contracted Party's assessment of the disclosure request, which SHOULD include:

1.7.1. Authenticated Requestor Name

1.7.2. Organization/Entity

1.7.3. Country/Jurisdiction

1.7.4. Email Address

1.7.5. Position/Title

1.7.6. Authentication Provider Name

1.7.7. Authentication Status

1.7.8. Authentication Time

1.7.9. Authentication Valid Until

1.7.10. Assertion Identifier

1.7.11. Token Issue Date/Time

1.7.12. Token Expiry Date/Time

1.7.13. Token Digital Signature

Note: The list provided in 1.7.1 - 1.7.13 MAY be further adjusted during implementation, in consultation with relevant stakeholders as appropriate, to provide flexibility, address changes in technology or security, etc. Relevant stakeholders means the IRT before the policy goes into effect and the Standing Committee, after the policy goes into effect.

Implementation Guidance

1.8. Per the RDRS Standing Committee's recommendation, initial implementation would begin with law enforcement. The recommendation is not meant to exclude other communities who wish to establish an Authentication Provider of their own. In the law enforcement example specifically, an Authentication Provider need not provide authentication services to all law enforcement agencies globally. It may serve a single law enforcement agency, a national organization representing multiple agencies, or a regional or international body, provided the entity satisfies ICANN's published requirements for Authentication Providers. This federated approach allows communities to decide whether the benefits of authentication justify the investment required to establish and operate an Authentication Provider of their own.

1.9. The SSAD SHOULD provide a mechanism through which each recognized Authentication Provider can make available its current requirements and procedures as required under Sections 1.3.1–1.3.5. Such mechanism MAY include a link provided by the Authentication Provider to a current description of those requirements and procedures. To support transparency and accountability, the SRT expects ICANN org or its designee to publish and

maintain a current list of recognized Authentication Providers, including the community or category of Requestors served by each.

1.10. The SRT recognizes that eligibility requirements may vary depending on the community or category of Requestors served by an Authentication Provider. The framework should therefore allow for eligibility criteria appropriate to the relevant community. For example, eligibility criteria for a law enforcement community or consumer protection agency may include evidence of current employment or official credentials, while eligibility criteria for a community of legal professionals may include evidence of a current professional license or similar qualification. The framework SHOULD provide sufficient flexibility to accommodate different types of Authentication Providers and the communities they serve, including allowing different approaches to meeting the requirements for eligibility verification, credential management, ongoing review, auditing and authentication attributes. Such flexibility should preserve the applicable minimum administrative, technical and security requirements, while allowing Authentication Providers to demonstrate how their procedures satisfy those requirements.

1.11. While the list of minimum authentication attributes provided in 1.7 is subject to adjustment during implementation, the SRT is providing the below guidance to assist in its understanding of what these elements mean:

- 1.7.1. **Authenticated Requestor Name:** The name of the individual that has been authenticated by the Authentication Provider and to whom the authentication is attributable.
- 1.7.2. **Organization/Entity**: The organization or entity with which the Authenticated Requestor is affiliated, as verified by the Authentication Provider.
- 1.7.3. **Country/Jurisdiction**: The country or jurisdiction associated with the Authenticated Requestor.
- 1.7.4. **Email Address**: The email address associated with the Authenticated Requestor.
- 1.7.5. **Position/Title**: The position, job title, or official role held by the Authenticated Requestor within the organization or entity with which they are affiliated, as verified by the Authentication Provider.
- 1.7.6. **Authentication Provider Name**: The name of the Authentication Provider that authenticated the requestor.
- 1.7.7. **Authentication Status:** An indication that the Requestor has successfully completed the Authentication Provider's applicable authentication procedures and is considered authenticated.
- 1.7.8. **Authentication Time**: The date and time at which the Authentication Provider established or confirmed the Requestor's authenticated status.
- 1.7.9. **Authentication Valid Until**: The date and time through which the Authentication Provider considers the Requestor's authenticated status to remain valid, subject to revocation or suspension.
- 1.7.10. **Assertion Identifier**: A unique identifier associated with the authentication assertion or authentication event represented by the Authentication Token.
- 1.7.11. **Token Issue Date/Time**: The date and time at which the Authentication Token or equivalent authentication assertion was issued. This attribute is distinct from the Authentication Time, which identifies when the Requestor's authenticated status was established or confirmed. The Token Issue Date/Time identifies when the particular token or assertion was generated or issued.
- 1.7.12. **Token Expiry Date/Time**: The date and time after which the Authentication Token should no longer be accepted as valid. This attribute is intended to limit the period

during which the token may be used and to reduce the risk associated with unauthorized reuse of a token.
- 1.7.13. **Token Digital Signature:** A cryptographic mechanism or equivalent security measure that enables the recipient of the Authentication Token to verify that the token was issued by the recognized Authentication Provider and that the token's contents have not been altered after issuance.

Recommendation Rationale

The EPDP Team envisioned a detailed accreditation system, involving the use and potential outsourcing of accreditation authorities. The accreditation system provided details on identity verification, additional assertions/credentials, application procedure, revocation procedure, dispute/complaints process, revocation of access, appeal mechanism, etc. The Operational Design Assessment forecasted a high cost associated with this detailed accreditation scheme for a global user base, that also required cost recovery, and, accordingly, the RDRS pilot tested a lighter weight system where users register to become a requestor, but are not accredited.

The RDRS Standing Committee ultimately recommended that this detailed accreditation system is not needed in order to proceed with the SSAD; however, the Standing Committee noted that ICANN org or its designee could allow for introduction of specific user authentication, and the RDRS Standing Committee recommended beginning with the authentication of law enforcement users.

The SRT reviewed the feedback from the RDRS Standing Committee and agrees with the finding that the cost associated with centrally accrediting all users justifies significantly paring down Recommendation 1 to remove mandatory accreditation of all users. Additionally, the SRT agrees with beginning with the authentication of law enforcement users. This Supplemental Recommendation, however, is not meant to deprecate or minimize the importance of requestor accountability when using the SSAD. Requestor accountability, and potential removal from the SSAD due to misuse or abuse, is contemplated in Supplemental Recommendations 6 and 7.

The RDRS Standing Committee noted, and the SRT agrees that additional requestor communities may become authenticated through recognized Authentication Providers, provided the Authentication Providers satisfy ICANN's published administrative, technical, and security requirements. The SRT notes its expectation that ICANN org or its designee would publish the requirements and review the applications for entities interested in becoming recognized Authentication Providers, but would not be responsible for identity proofing, as that responsibility lies with the recognized Authentication Provider. This partially aligns with the original SSAD concept of additional assertions/credentials, but endeavors to outsource, scale, and incrementally implement authentication for communities who feel this is needed.

The SRT also considered the relationship between Supplemental Recommendation 1 and Implementation Note K of the Registration Data Policy, which provides that the obligations under Section 10.7 concerning Urgent Requests for Lawful Disclosure become effective upon the policy effective date of the Consensus Policy establishing a process for authentication of requestors. The SRT considers the SSAD Supplemental Recommendations, if adopted by the ICANN Board and implemented, including the implementation of an operational mechanism for Authentication, to satisfy the condition identified in Implementation Note K without requiring a separate policy development process. For the avoidance of doubt, the SRT's recommendations

do not prescribe a particular technical mechanism for Authentication or preclude future policy work to enhance or modify the Authentication process. Lastly, the SRT does not intend for the future expansion of Authentication to additional requestor communities, beyond those contemplated for initial implementation, to delay satisfaction of the condition specified in Implementation Note K.

Supplemental Recommendation 2 [3]: Criteria and Content of Requests

Supplemental Recommendation 2 was formerly numbered as Recommendation 3 under the original EPDP Phase 2 SSAD recommendations. Supplemental Recommendation 2 also includes text from the original SSAD Recommendation 2 and 7.

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

2.2. The SRT recommends that each SSAD request MUST include all information necessary for a disclosure decision, including, at a minimum, the following information:

2.2.1. Domain name pertaining to the request for access/disclosure;

2.2.2. Requestor's identity and who they are acting on behalf of (if applicable)

2.2.3. Where applicable, an Authentication Token;

2.2.4. Information about the legal rights of the Requestor specific to the request and legitimate interest or other lawful basis and/or justification for the request, (e.g., What is the legitimate interest or other lawful basis; Provide a brief description of the specific issue the request is attempting to resolve.);

2.2.5. Affirmation that the request is being made in good faith and that data received (if any) will be processed lawfully in a manner that respects internationally recognized human rights and only in accordance with the purpose specified in 2.2.4;

2.2.6. A list of data elements requested by the Requestor, and why the data elements requested are necessary for the purpose of the request;

2.2.7. Whether the requestor is seeking the underlying customer data for a domain using privacy or proxy services. The SSAD MUST allow the Requestor to indicate that it is unknown whether a privacy or proxy service is in use where this cannot reasonably be determined from available registration data;

2.2.8. Request type (e.g., Urgent – see also Supplemental Recommendation #4 - Request Types and Service Level Agreements – see also Supplemental Recommendation #5 - Contracted Party Disclosure Decision).

2.3. The SSAD MUST confirm that all required fields have been filled out. It SHOULD not be possible for a Requestor to submit a request that is incomplete. In this context, SSAD means the SSAD system and/or the operator of SSAD, as the case may be.

Implementation Guidance

The SRT expects that:

2.4. Each request must include the information detailed in Section 2.2 above. While the mechanism to collect and place this data into a request (be it a web form, an API or similar) is not specified by this policy, the offering of pre-populated fields, tick boxes and/or dropdown options should be considered. However, the use of pre-populated fields, tick boxes or dropdown options must not exclude the ability of Requestors from submitting free form responses.

2.5. Requests must be in English unless the Contracted Party that is receiving the request indicates they are also willing to receive the request and/or supporting documents in other language(s). In cases where the Contracted Party accepts languages in addition to English, in the event of a discrepancy, the English version shall be considered authoritative.

2.6. With respect to 2.2.4, the requestor may request nonpublic data for the exercise of their public policy tasks, including but not limited to civil and criminal law enforcement authorities, data protection and regulatory authorities, judicial authorities, consumer rights organizations granted a public policy task by law or delegation from a governmental entity, cybersecurity authorities granted a public policy task by law or delegation from a governmental entity including national Computer Emergency Response Teams (CERTs). The requestor may also request data for specific purposes not limited to (i) criminal law enforcement, national or public security, (ii) non law enforcement investigations and civil claims, including intellectual property infringement and UDRP and URS claims, (iii) consumer protection, abuse prevention and network security, (iv) obligations applicable to regulated entities, or to (v) verify a registrant's claim of ownership of a domain name registration. These specific examples were included in the original EPDP Phase 2 recommendations (Recommendations 2 and 7), and the SRT believes it is important to preserve them for additional context during the implementation of this policy for the purposes of improving the SSAD request form and for the purposes of logging and reporting on information related to the request type, e.g., consumer protection, IP, litigation, etc.

2.7. The purposes listed in 2.6 represent a non-exhaustive list. Accordingly, the SSAD request form SHOULD allow for a free-form field (or similar) that allows a requestor to specify if their purpose is not listed as part of the dropdown list.

2.8. For the avoidance of doubt, identification of a requestor category or purpose described above does not, by itself, establish an entitlement to disclosure or predetermine the outcome of the Contracted Party's evaluation of the request under these recommendations.

2.9. The policy SHOULD allow for flexibility in implementation, such that required content and format of requests can evolve over time as specified by ICANN, which SHOULD involve consultation with the Implementation Review Team (prior to SSAD launch) or SSAD Standing Committee (post SSAD launch), before any changes are made to required contents of requests.

2.10. During implementation, ICANN org SHOULD solicit feedback from interested stakeholders, including, for example, Requestors, Contracted Parties, registrants to ensure the form is both user-friendly and fit for purpose.

2.11. The SRT notes the SSAD SHOULD enable a Contracted Party to provide information concerning how it handles SSAD requests for underlying privacy or proxy customer data, including:

> (i) whether it is willing to consider disclosure of underlying privacy/proxy customer data in response to an SSAD request where it holds or has access to the underlying data;
>
> (ii) information regarding any types of additional information or documentation that may be relevant to the Registrar's review of an SSAD request for underlying privacy or proxy customer data;
>
> (iii) whether the Registrar's ability and/or willingness to evaluate a specific request for disclosure of underlying privacy/proxy customer data depends on any additional factors that are specific to a request (for example, if a Registrar sponsors domains for which privacy/proxy services are provided by multiple service providers, will the Registrar consider requests for the underlying customer data for all such domains, or only domains for which the privacy/proxy service is provided by the Registrar or a Registrar Affiliate, rather than a third-party service provider);
>
> (iv) whether there is a mechanism for a requestor to identify if any exclusions identified in (iii) above can be determined by a requestor prior to submitting a request; and
>
> (v) where the request cannot be processed through the SSAD, the appropriate next step or submission channel.

This information SHOULD be accessible to requestors prior to the submission of an SSAD request. In other words, it should be clear to a requestor if the Registrar is willing to consider permissive disclosure of underlying data under Supplemental Recommendation 5.7.3. For the avoidance of doubt, such indication does not constitute a determination that disclosure will be made in response to any particular request, and each SSAD request remains subject to the Registrar's review and determination under this Policy.

Additionally, nothing in Supplemental Recommendation 2.11 modifies the requirements in Supplemental Recommendation 5 for Contracted Parties to review and evaluate all SSAD requests.

Where the use of a privacy or proxy service can be determined from authoritative registration data or other information made available pursuant to applicable Consensus Policy, the SSAD MUST make that information available to the Requestor.

2.12. With regards to Supplemental Recommendation 2.2.3, authenticated requestors SHOULD be able to include an Authentication Token when submitting either an Urgent Request or Standard Request.

Recommendation Rationale

Supplemental Recommendation 2 is designed to standardize the SSAD request form and form requirements to ensure (i) predictability for requestors, e.g., requestors know what is needed by the SSAD to submit requests, and (ii) the data points needed for Contracted Parties to properly

evaluate a request are provided in the initial submission. The added implementation guidance in 2.10 was included because the RDRS Standing Committee believed additional input is needed in implementation to ensure that the standard request form is in plain English and meets the needs of both requestors and the Contracted Party.

Supplemental Recommendation 3 [4]: Acknowledgement of Receipt and Relay of the Disclosure Request

Supplemental Recommendation 3 was formerly numbered as Recommendation 4 under the original EPDP Phase 2 SSAD recommendations. Supplemental Recommendation 4 also incorporates text from the original SSAD Recommendation 9.

3.1 Acknowledgement of receipt

3.1.1. Following confirmation that all required fields have been filled out and the requestor's submission of the request, the SSAD MUST immediately and synchronously respond with the acknowledgement of receipt and relay the disclosure request to the responsible Contracted Party.

3.1.2. The response provided by the SSAD to the Requestor SHOULD also include information about the subsequent steps, information on how public registration data can be obtained as well as the expected timeline consistent with the SLAs outlined in Supplemental Recommendation 4.

3.2. Relay of disclosure request

3.2.1. By default, the SSAD MUST relay the disclosure request to the Registrar of Record. Where a Registry Operator has agreed to participate in the SSAD and has notified SSAD/ICANN org or its designee that it is willing to receive disclosure requests for names under its management, the SSAD MUST provide the Requestor, prior to submission, a clear choice of whether to route the request to (a) the Registrar of Record, (b) the Registry Operator, or (c) both. A Registry Operator's voluntary election to receive SSAD requests under this provision does not, by itself, alter the substantive disclosure obligations applicable to the Registry Operator or the Registrar of Record under these recommendations or applicable policy.

Implementation Guidance

The SRT expects that:

3.3. The acknowledgement of receipt will include a "ticket number" or similar mechanism to facilitate interactions between the Requestor and the SSAD, details to be worked out in implementation.

3.4. The SSAD relays the disclosure request as well as necessary and appropriate information about the Requestor to the Contracted Party.

3.5. The SSAD SHOULD include functionality that allows Requestors and Contracted Parties to access and track the status of SSAD requests. For Requestors, this SHOULD include a user interface and an API through which requests may be submitted and their status tracked (for example, under review, on hold, or priority level changed). For Contracted Parties, the SSAD SHOULD provide both a user interface and an API to access all SSAD functionality and track requests with an active, paused, or completed SLA.

During implementation, the SRT expects ICANN org to consult with interested stakeholders regarding the implementation of these features, including onboarding considerations. Additionally, the SRT expects ICANN org to provide Contracted Parties with a sufficient opportunity to test and operationalize their use of the API. Contracted Parties have noted that 18 months may be needed, but the timeline will be discussed during implementation.

3.6. The SSAD SHOULD allow for a ccTLD operator who uses RDAP to voluntarily opt into participation in the SSAD with the mechanics to be worked out in implementation to meet the purpose of this Supplemental Recommendation 3.6.

> 3.6.1. ccTLD support SHOULD NOT be considered required functionality for the initial launch of the SSAD and MAY be added as part of a later phase of Implementation.
>
> 3.6.2. The SSAD MAY establish baseline requirements for ccTLD operators to participate in the SSAD (for example, RDAP MUST be supported).
>
> 3.6.3. In implementing ccTLD support, ccTLD operators SHOULD be consulted to ensure the implementation feasibly supports ccTLD operator participation.

3.7. For participating Registry Operators under 3.2.1, the SSAD SHOULD provide the ability for Registry Operators to indicate available data elements for domain names under their management. This information SHOULD be made available to Requestors prior to the submission of a disclosure request and does not constitute a representation that this data be disclosed in response to a request.

Recommendation Rationale

Supplemental Recommendation 3 specifies how SSAD requests are received by the system and routed to the correct entity (generally, the Registrar of Record) to ensure the appropriate entity receives the request. Additionally, Supplemental Recommendation 3 specifies explanations and tracking abilities provided to educate the Requestor on what to expect.

The SRT adjusted 3.4 to remove disclosure requests for which automated processing of the disclosure decision applies due to guidance from the RDRS Standing Committee. The RDRS Standing Committee noted “full automation is currently infeasible due to the need for nuanced human judgment in balancing privacy and disclosure rights”.

To be clear, this does not mean to restrict a Contracted Party from choosing to automate disclosure of nonpublic registration data; however, the SRT notes that due to cost and complexity, the SRT is not recommending the SSAD to direct Contracted Parties to automatically disclose nonpublic registration data.

The SRT considered the scenario where the ccTLD operator opts in to the SSAD indicating that disclosure requests should go to the ccTLD operator directly. The SRT understands that ccTLD implementations vary and based on ccTLD operators feedback, implementation MAY differ.

Supplemental Recommendation 4 [6]: Request Types and Service Level Agreements

Supplemental Recommendation 4 was formerly numbered as Recommendation 6 under the original EPDP Phase 2 SSAD recommendations. Supplemental Recommendation 4 also incorporates text from the original SSAD Recommendation 10.

Request Types

4.1 The SRT recommends that the SSAD accommodate at least the following two (2) request types: Urgent Requests and Standard Requests, as described below.

Urgent Requests

4.1.1. Urgent Requests under the SSAD are defined in accordance with Section 3.8 of the Registration Data Policy, including both the definition of "Urgent Requests for Lawful Disclosure"[5] and the accompanying definition of "critical infrastructure."[6] Any subsequent amendments to either definition in the Registration Data Policy SHALL apply correspondingly to this Recommendation, ensuring continued consistency between the two policies.

4.1.1.1. Upon receipt of an Urgent Request from the SSAD, Contracted Party MUST:

4.1.1.1.1. Acknowledge receipt of the Urgent Request within two hours; and

4.1.1.1.2. Respond to the Urgent Request without undue delay, not to exceed 24 hours absent exceptional circumstances as described in 4.1.1.1.3.

4.1.1.1.3. If exceptional circumstances occur, Registrar and Registry Operator MUST, without undue delay and in all cases within 24 hours, notify the Authenticated Requestor if there is a need for an extension to respond. The notification MUST include the rationale for the extension and the timeframe within which the Registrar or Registry Operator expects to respond, which cannot exceed 72 hours from receipt of the request.

Examples of exceptional circumstances include events of force majeure (unforeseen and uncontrollable events), such as those affecting the availability of the infrastructure, and circumstances associated with the complexity of the request, such as a request involving a high number of domain names. For the avoidance of doubt, circumstances which do not justify extending the 24-hour

[5] Urgent Requests for Lawful Disclosure" ("Urgent Requests") are a subset of Disclosure Requests submitted by an Authenticated Requestor that are limited to circumstances that pose an imminent threat to life, of serious bodily injury, to critical infrastructure, or of child exploitation in cases where disclosure of the data is necessary in combatting or addressing this threat.
[6] Critical infrastructure means the physical and cyber systems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety.

timeline include foreseeable circumstances such as calendar holidays, planned leave, or planned travel.

4.1.2. The Contracted Party MUST maintain a designated contact for dealing with Urgent Requests submitted via the SSAD which can be confidentially and securely stored by the SSAD. Due to the potential for abuse, the designated contact MUST NOT be made public. When Urgent Requests are submitted via the SSAD, in addition to standard request routing, the SSAD MUST also notify the designated contact that an Urgent Request has been submitted.

Standard Requests

4.1.3. Standard Requests**:** All other requests.

4.1.3.1. Upon receipt of a Standard Request from the SSAD, Contracted Party MUST:

4.1.3.1.1. Acknowledge receipt of the Standard Request without undue delay, not to exceed two (2) business days from receipt; and;

4.1.3.1.2. Respond to the Standard Request without undue delay, but no more than thirty (30) calendar days from acknowledgement absent exceptional circumstances as described in 4.1.1.1.3.

Summary of Response Times (SLAs) for SSAD requests

Request Type	SLA
Urgent Requests from an Authenticated Requestor	24 hours
Standard Requests **(**All other requests)	720 hours (30 days)

4.2. For Standard Requests, Requestors MUST have the ability to indicate that the disclosure request concerns consumer protection, e.g., an issue involving phishing, malware or fraud, in which case the Contracted Party SHOULD prioritize the request over other Standard Requests.

Recategorization of Request Type

4.3. The Contracted Party MAY recategorize the request type during the review of the request in instances where the Contracted Party reasonably believes the proposed request type does not

meet the definitions described in 4.1.1 and 4.1.3.[7] When reassigning the request type, the Contracted Party MUST provide a rationale to the requestor for its reassignment.

SLA Calculation

4.4. For purposes of calculating SLA response time, the SRT recommends the SLA starts when a complete request with all supporting information is provided to the Contracted Party by the SSAD. The SLA stops when the Contracted Party:

> 4.4.1. Responds to the Requestor with (a) the information requested, (b) a rejection response, (c) or a request for additional information; and
>
> 4.4.2. Indicates the outcome (approved, denied, ICANN review, or additional information needed) via the SSAD.

4.5. A reexamination request (as described in 5.9 and 5.10) would be considered the start of a new SSAD request for SLA calculation purposes. The Contracted Party MUST treat the updated SSAD request as a continuation of the original SSAD request and SHOULD prioritize the reexamination request.

4.6. A requestor response with more information further to 5.4 would be considered the start of a new SSAD request for SLA calculation purposes. For the avoidance of doubt, when a Contracted Party provides the requestor with the outcome “additional information needed”, the SLA calculation is stopped. If and when the requestor provides additional information through a new SSAD request, a new SLA calculation starts. (Please see Implementation Guidance 4.13.) The Contracted Party MUST treat the updated SSAD request as a continuation of the original SSAD request and SHOULD prioritize the request.

4.7. The SRT recommends that Contracted Parties MUST publish their standard business hours, business days, and accompanying time zone in the SSAD portal.

Implementation Guidance

Recategorization of Request Type

4.8. The SRT expects the SSAD to provide functionality for the Contracted Party to (i) recategorize the request type provided by the requestor and (ii) provide a rationale for the recategorization. When a Contracted Party recategorizes a request, the SRT expects the SSAD to trigger an immediate notification to the requestor, which includes the rationale provided by the Contracted Party.

4.9. If an Urgent Request is recategorized to Standard, requestors SHOULD have a one-time opportunity to provide additional rationale, clarification, or supporting information to support restoration of the request to Urgent status. Any such information SHOULD be submitted within 24 hours of receiving the notice of recategorization. The SRT expects the SSAD to notify the

[7] For example, the Contracted Party may note that although the **Request Type** is set as Urgent Request, the request shows no evidence documenting an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation and accordingly, the request should be recategorized.

Contracted Party immediately when the requestor submits additional supporting information. Upon receipt of that information, the SLA associated with the original Urgent Request MUST be reset and begin again.

4.10. Improper recategorization: If a Requestor is of the view that its request was improperly recategorized, the Requestor MAY file a complaint with ICANN Org. ICANN Org will then investigate the Contracted Party's compliance with the applicable requirements of this Policy under its standard enforcement processes.

SLAs

4.11. In discussing the current SLA under the Registration Data Policy, the SRT noted that the actual response times in the RDRS were significantly below 30 days, and in order to encourage Requestors to use the SSAD, it will be important to publicize the actual response times so that prospective requestors are informed the 30-day response time is the longest possible response time but does not represent the average.

4.12. Where there may be a delay between communicating the response to the requestor and recording the outcome in the SSAD system, the SSAD system SHOULD allow the Contracted Party to modify the recorded response date and time to reflect the actual time the response was provided to the Requestor. The SSAD system SHOULD restrict the date and time adjustment period to prevent an adjustment that is not within the response time from the date of request submission required for Urgent Requests and Standard Requests.

4.13. In instances where a requestor chooses to provide additional information in response to a Contracted Party’s determination that additional information is needed, the SRT expects the SSAD system to allow for a Requestor to duplicate the previous request and submit additional information within the duplicate request, instead of reentering the same information into a new request. The SSAD system SHOULD provide the requestor with a field to include the original request tracking information.

4.14. Further to 4.7, the SRT expects the SSAD to provide the functionality to allow Contracted Parties to publish their standard business hours, business days, and accompanying time zone.

4.15. A non-exhaustive list of issues potentially related to consumer protection includes phishing, malware, fraud, or other deceptive behaviour. For example, the use of a domain name to mislead, impersonate, or otherwise deceive users for a harmful purpose, such as obtaining sensitive information or depriving a victim of assets, would raise consumer protection concerns.

Recommendation Rationale

In the very rare instance where access to registration data is needed urgently in response to an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation, Supplemental Recommendation 4 provides the definitional requirements for meeting this rare threshold. The SRT elected to match the definition in the Registration Data Policy so that this definition would be consistent across the two policies. Because of the short response timeframe (defined in Supplemental Recommendation 4), the SRT noted the need for consequences for abusing this flag. In addition to there being consequences for requestors abusing the Priority 1 (Urgent Request) flag, the SRT also highlighted that if a requestor

believes a Contracted Party improperly re-categorizes a request, that requestor may file a complaint with ICANN Compliance, and this would be investigated according to ICANN's standard contractual compliance process. The SRT discussed the original Priority 2 Level, which was reserved for ICANN administrative proceedings, but due to discussions outside of this group on how to mitigate against false ICANN administrative claims, the SRT ultimately decided to remove the separate category from Supplemental Recommendation 4. In removing the ICANN administrative proceedings category, the SRT noted two things: (1) the response times required under existing Consensus Policies, e.g., 2 business days for responding to UDRP registrar verification requests, remain in place and are NOT affected by the SLAs under this policy, and (ii) the SRT is not intending to restrict the use of SSAD for administrative proceedings in the future - instead, this could be an item for discussion in the SSAD Standing Committee described in Supplemental Recommendation 12.

Supplemental Recommendation 5 [8]: Contracted Party Disclosure Decision

Supplemental Recommendation 5 was formerly numbered as Recommendation 8 under the original EPDP Phase 2 SSAD recommendations. Supplemental Recommendation 5 also incorporates text from the original SSAD Recommendation 5 and 12.

General requirements

Following receipt of a request from the SSAD,:

5.1. The Contracted Party MAY engage a third party to perform the review and disclosure determination. However, where a third party performs this function, the Contracted Party remains responsible for ensuring compliance with all applicable requirements of this Policy.

Review of SSAD Disclosure Request

5.2. The Contracted Party, or a third party acting on its behalf, MUST review each disclosure request on its merits and determine whether it can lawfully disclose the requested data, including underlying privacy or proxy customer data where requested. The review and response MUST be consistent with the Registration Data Policy.

Decision to Disclose following Review of SSAD Request

5.3. Following its review under Section 5.2, the Contracted Party MUST respond to the disclosure request by either:

(i) providing the requested data, in whole or in part;
(ii) denying disclosure, in whole or in part, and providing a rationale in accordance with Section 5.5; or
(iii) requesting additional information or documentation in accordance with Section 5.4.

Additional Information of Documentation

5.4 If the Contracted Party determines the request is incomplete or additional information or documentation is needed to make a determination, the Contracted Party MUST notify the Requestor, indicate the specific additional information or documentation required, and provide the Requestor an opportunity to submit further information prior to making a determination. The

submission of additional information and calculation of response times are governed by Supplemental Recommendation 4.

Denial, in Whole or in Part

5.5. If the Contracted Party denies disclosure, in whole or in part, it MUST provide a rationale meeting the requirements of Section 10.6.2 of the Registration Data Policy. Where the Contracted Party cannot provide the requested underlying privacy or proxy customer data because it does not hold or have access to that data, the response MUST clearly state this. Where the Contracted Party is aware of an alternative channel through which the Requestor may submit its request, the Contracted Party MUST provide information sufficient to identify that channel.

5.6. Absent any legal requirements to the contrary, the Contracted Party MUST NOT deny a request solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement or the investigation of intellectual property infringement.

Registration Data that MAY be Disclosed

Disclosure, in Whole or in Part

5.7. In the event the Contracted Party discloses data further to Section 5.3, the SRT recommends Contracted Parties:

> 5.7.1. SHOULD only disclose the data elements requested by the Requestor or a subset thereof;
>
> 5.7.2. MUST return current data or a subset thereof (no historic data);
>
> 5.7.3. Where a disclosure request concerns a domain registered through a privacy or proxy service, the Contracted Party MUST ensure the request is evaluated and responded to in accordance with this Recommendation and any applicable requirements of the Consensus Policy on privacy/proxy registrations.

5.8. A Contracted Party MUST NOT take action with respect to the subject domain name (including suspension, repossession, transfer to the Contracted Party itself, or deletion) for the purpose of mooting its obligation to respond to a pending SSAD disclosure request. Where a Contracted Party takes such action based upon information supplied in a disclosure request, it MUST notify the Requestor of its actions and MUST still respond to the disclosure request on the merits as to the data that existed at the time of the request.

Reexamination Request

The Requestor:

5.9. MAY file a reexamination request with the Contracted Party through the SSAD if it believes its request was improperly denied. For the avoidance of doubt, as noted in Supplemental Recommendation 4.5 a reexamination request is treated as a new SSAD request for SLA purposes.

5.10. MUST, within its reexamination request, provide a supporting rationale as to why its request must be reexamined. The supporting rationale should provide sufficient detail as to why the Requestor believes its request was improperly denied.

5.11. MAY, if a Requestor believes a Contracted Party is not complying with any of the requirements of this policy, file a complaint with ICANN Org. ICANN Org will then investigate complaints of lack of compliance with the requirements of the SSAD policy obligations under its standard enforcement processes.

Implementation Guidance

5.12. The SRT envisions the Contracted Party having the ability to communicate with the Requestor via a dedicated ticket (or two-way communication feature/functionality) in the SSAD. The SRT also envisions the SSAD to be protected by industry-standard technical and organizational security measures, including encryption, to protect the transmission of Personal Data, in accordance with applicable data protection laws and cyber security acts. In implementing this two-way communication feature, ICANN org or its designee MUST ensure the SSAD has mechanisms to accept and address data subject access requests.

5.13. Current data means the data reviewed by the Contracted Party when making the determination whether to disclose the data. In order to lower the possibility of changes to the data during the pendency of an outstanding disclosure request, e.g., if the registrant updates its contact data, Contracted Parties are encouraged to disclose data as soon as possible following its decision on whether to disclose. For the avoidance of doubt, historic data refers to the registration data in place before the request for disclosure was made, not registration data that may have changed as a result of any updates made by the registrant between the time the request for disclosure is reviewed and the decision to disclose the registration data

5.14. The SSAD SHOULD provide functionality for a Requestor to submit a reexamination request and SHOULD clearly identify the submission to the Contracted Party as a reexamination request, including the relevant prior SSAD ticket number(s). The Requestor SHOULD be provided the opportunity to submit any additional information or documentation it believes should be considered as part of the reexamination

Recommendation Rationale

Supplemental Recommendation 5 explains the requirements for Contracted Parties to review each request received through the SSAD and recognizes that the Contracted Party has the ultimate authority to approve or deny a request because the Contracted Party bears the risk and liability associated with improperly disclosing personal data.

Contracted Parties are, however, required to respond to every SSAD request. Following review, the Contracted Party must either provide the requested data, in whole or in part; deny disclosure, in whole or in part, and provide the required rationale; or request additional information or documentation. Where a request is denied, the Contracted Party is required to provide a sufficiently specific rationale for the denial. A meaningful rationale can help the Requestor understand the basis for the decision and, where appropriate, improve future

requests, providing greater predictability and mutual benefit to Requestors and Contracted Parties.

The original recommendation included a number of requirements derived from the GDPR. While these requirements MAY apply in some circumstances, they also MAY NOT apply and should not be required where they do not. Accordingly, specific GDPR-based language was removed to avoid confusion in implementation, including issues observed during the RDRS pilot. For clarity, removal of this language DOES NOT limit a Contracted Party's ability or responsibility to conduct its own review under the relevant legal framework; rather, it is intended to avoid enshrining or interpreting a particular law through Consensus Policy.

During ICANN87, the SRT considered additional legal, policy and implementation concerns regarding the interaction between Supplemental Recommendation 5 and the Registration Data Policy (RDP), including the potential for overlapping or different requirements to apply to substantially the same disclosure process depending on how a request is submitted. Concerns were also raised regarding provisions that could require ICANN org to interpret or enforce legal standards that remain part of the Contracted Party's substantive disclosure determination.

In response, the SRT further streamlined Supplemental Recommendation 5 and aligned it more closely with the existing RDP framework. Where the RDP or other applicable Consensus Policy already addresses an element of the disclosure process, Supplemental Recommendation 5 references or relies on that framework rather than establishing a parallel or potentially inconsistent requirement. At the same time, the Supplemental Recommendation retains the SSAD-specific requirements necessary to provide a clear and usable process, including the handling of additional information, rationales for denial, privacy/proxy requests, current data and reexamination requests.

The SRT gave particular consideration to requests involving privacy or proxy services. Such requests remain subject to review and response under Supplemental Recommendation 5, together with any applicable requirements of the Consensus Policy governing privacy/proxy registrations (currently under development). This approach is intended to preserve a meaningful pathway for SSAD requests without creating an independent obligation to disclose underlying privacy or proxy customer data.

Supplemental Recommendation 6 [11]: SSAD Agreements and Policies

Supplemental Recommendation 6 was formerly numbered as Recommendation 11 under the original EPDP Phase 2 SSAD recommendations.

6.1. The SRT recommends that minimum expectations for appropriate agreements and policies, such as terms and conditions for the SSAD, an SSAD privacy policy, disclosure agreement, and an acceptable use policy are further defined during the implementation phase, to be subsequently developed and enforced by the entity responsible for the SSAD (by ICANN Org or a third party that has been tasked by ICANN Org to take on this enforcement function). These agreements and policies MUST take into account all recommendations from this policy. These agreements and policies are expected to be developed and negotiated, as appropriate, by the parties involved in SSAD, taking the below implementation guidance into account.

Updates to SSAD Terms and Conditions

6.2. ICANN org MUST review or coordinate the review of the SSAD Agreements and Policies at regular intervals, precise timing of reviews to be determined during implementation. The SSAD Agreements and Policies MAY be updated, as appropriate, to address applicable law and human rights practices, including global data protection standards, and operational security or stability needs. Where ICANN org is responsible for such updates and they materially affect obligations of requestors or Contracted Parties, ICANN org MUST consult the community via the SSAD Standing Committee prior to implementation, unless doing so would prevent or delay ICANN org from complying with applicable law or other binding legal or regulatory requirements, or from taking action necessary to address security or stability needs.

Implementation Guidance

6.3. Privacy Policy for processing of personal data of SSAD Users (SSAD Requestors and Contracted Parties) by SSAD

The SRT recommends, at a minimum, the Privacy Policy MUST include information about data processing and privacy, including but not limited to:

- 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
- Transparency requirements
- Data security requirements
- Accountability measures (privacy by design, by default, Data Protection Officer (DPO) above certain size, etc)

6.4. Terms and Conditions for SSAD users (SSAD Requestors and Contracted Parties)

The SRT recommends, at a minimum, the Terms and Conditions MUST address the following:

- Requestors are responsible for damages or costs related to third party claims arising from (i) their misrepresentations in the authentication or request process; or (ii) misuse of the requested data in violation of the applicable terms and conditions or applicable law(s).
- Nothing in these terms limits any parties' liability or rights of recovery under applicable civil or criminal laws (i.e. Requestors are not precluded from seeking recovery from controllers where those rights are provided under law).
- Nothing in these terms shall be construed to create indemnification obligations for public authority Requestors who lack the legal authority to enter into such indemnification

clauses. Further, nothing in this clause shall alter potentially existing government liability as a recourse for the operators of the SSAD.
- Data request requirements
- Logging and audit requirements sufficient to support security investigations, including retention of request metadata, purpose statements, and disclosure decisions for a minimum period aligned with Supplemental Recommendations 9 and 10 and operational security needs
- Ability to demonstrate compliance and to provide timely access to logs to accredited security researchers / LEA under lawful process
- Applicable prohibitions
- Abuse prevention requirements (including technical and procedural measures to detect, report, and deter bulk, automated, or bad-faith requesting; mandatory cooperation with SSAD Misuse Investigator)

6.5. Disclosure agreements for SSAD Requestors

The SRT recommends, at a minimum, SSAD Agreements and Policies MUST specify the use and retention requirements applicable to Requestors in cases where the requested data is disclosed to the Requestor:
- 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 and destruction of data: 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, unless otherwise required to retain such data for a longer period under applicable law.
- Lawful use of data

The SRT notes ICANN org may consider an approach similar to the RDRS, whereby ICANN org provides a standard disclosure agreement that Contracted Parties may use, while allowing Contracted Parties to replace or supplement that agreement with their own terms, as appropriate.

6.6. Acceptable Use Policy for SSAD Requestors.

The Requestor MUST accept the Acceptable Use Policy before disclosure requests can be submitted through SSAD.

At a minimum, the Acceptable Use Policy MUST include the following requirements:

The Requestor:

6.6.1. MUST only request data from the current RDS data set (no historic data);

6.6.2. MUST, for each request for RDS data, provide representations of the corresponding purpose and lawful basis or other authorization under applicable law for the processing, which will be subject to auditing (see the Supplemental Recommendation10: Auditing for further details);

6.6.3. MAY request data from the SSAD for multiple purposes per request, for the same

set of data requested;

6.6.4. 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). When multiple purposes are stated, each purpose must independently satisfy the representation and auditing requirements; a single request may not be used to 'bootstrap' an unrelated purpose.

6.6.5. MUST provide an affirmation that the request is being made in good faith.

These representations will be subject to auditing (see Supplemental Recommendation 10: Auditing further details).

6.7. Consequences for Violating SSAD Agreements and Policies

6.7.1. Requestors MUST acknowledge that misuse or violation of SSAD Agreements and Policies may result in immediate suspension or revocation of access to the SSAD and may be considered an aggravating factor in request type handling or query-policy enforcement (cross-reference Supplemental Recommendations 4 and 7).

6.7.2. In the event a requestor violates the terms of use of SSAD Agreements and Policies, ICANN org or its designee MAY take measures such as (i) limiting the requestor's ability to submit requests through the SSAD, (ii) temporarily suspending the ability of a requestor to submit requests, or (iii) revoking a requestor's access to the SSAD. As noted above in Section 6.4, while this section defines what ICANN org MAY do in response to an SSAD Terms and Conditions violation, this section is not meant to restrict any parties' ability to seek rights of recovery under applicable law. Please see Supplemental Recommendation 7 for more information regarding expectation for notifying ICANN org regarding a potential violation.

6.7.3. ICANN org or its designee MUST maintain a public register of enforcement actions taken for violations of SSAD Agreements and Policies, redacted as necessary for privacy/LEA sensitivity.

6.8. The SRT is providing the following table to clarify its understanding of the agreements and policies referenced within this Recommendation. The agreements and policies described below may take different forms and may be structured, combined, or incorporated into other agreements or policies as appropriate during implementation, provided that the applicable requirements of this Recommendation are addressed.

Agreement or Policy: What?	**Purpose: Why?**	**Parties: Who?**
SSAD Terms and Conditions	Governs SSAD user's access to and use of the SSAD, e.g., account use, request submission, representations, misuse, etc.	ICANN org (or designee) and Requestors, Contracted Parties

SSAD Privacy Policy	Policy to explain how the SSAD processes personal data relating to users of the SSAD	ICANN org (or designee) and SSAD users/data subjects
Disclosure Agreement	Governs obligations associated with data disclosed in response to an SSAD request, e.g., retention, destruction, etc.	Requestors and Contracted Parties
Acceptable Use Policy	Governs obligations associated with permitted/prohibited conduct when using the SSAD, including requestor behavior and abuse prevention	ICANN org (or designee) and Requestors

Recommendation Rationale

Supplemental Recommendation 6 ensures SSAD users are responsible for important terms and conditions if they would like to make disclosure requests using the SSAD. These terms and conditions, including but not limited to an Acceptable Use Policy and a Privacy Policy, define acceptable behavior, specify important protections, and prevent misuse and abuse. Additionally, these terms are essential to ensure that the SSAD does not itself become a vector for abuse or a single point of failure for security investigations. These terms and conditions were an important part of the RDRS pilot, and further to the RDRS Standing Committee's guidance, the SRT recommends keeping these important terms and conditions in place.

Supplemental Recommendation 7 [13]: Query Abuse Policy

Supplemental Recommendation 7 was formerly numbered as Recommendation 13 under the original EPDP Phase 2 SSAD recommendations.

7.1. The SRT recommends that ICANN org or its designee:

7.1.1. MUST provide a mechanism for Contracted Parties to report perceived abusive requestors/requests.

7.1.2. Upon receiving a Contracted Party's substantiated report of suspected abusive use of the SSAD by a Requestor MUST stop the Contracted Party's SLA as described in Supplemental Recommendation 4 with respect to the reported request(s) and MAY stop the Contracted Party's SLA for other requests from the same Requestor while ICANN org or its designee investigates the report.

7.1.3. If, after receiving a report of abuse from a Contracted Party, ICANN org or its designee determines that a requestor has engaged in Abusive use of the SSAD, it

SHOULD take appropriate action, including limiting the number of requests by the same Requestor, revoking a Requestor's access to the SSAD, or suspending a Requestor's access to the SSAD;

"Abusive" use of SSAD MAY include (but is not limited to) one or more of the following behaviors/practices:

7.1.3.1. Repeated submission of requests using the wrong priority level, after the Requestor has been notified of the applicable criteria and the reasons for recategorization pursuant to Supplemental Recommendation 4.3.

7.1.3.2. High volume[8] automated submissions of malformed or incomplete requests.[9]

7.1.3.3. High volume automated duplicate requests that are frivolous, malicious, or vexatious[10].

7.1.3.4. Use of false, stolen, or counterfeit credentials to access the system.

7.1.3.5. 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.

7.1.4. A Requestor subject to an action under Section 7.1.3 MAY seek redress via ICANN org if it believes the action is unjustified.

7.2. The SRT recommends that Contracted Parties:

7.2.1. MUST NOT reject disclosure requests from SSAD system on the basis of abusive behavior which has not been determined abusive by ICANN org or its designee as described in sections 7.1.3.1 - 7.1.3.5 above, following its review of the Contracted Party's report of abuse. The SSAD Standing Committee described in Supplemental Recommendation 12 SHOULD review the abuse process and reporting structure of the SSAD after one (1) year of operation and recommend adjustments, as appropriate.

Implementation Guidance

7.3. The SRT recommends the SSAD MUST:

7.3.1. Support requests for fully qualified domain names (without wildcards).

[8] The SRT expects that "high volume" will be further defined in the implementation phase.
[9] As described in Implementation Guidance 7.1.3, the SRT recommends the focus group consider including explanatory language or tool tips to assist Requestors in submitting proper requests. While this will not eliminate malformed or incomplete requests, the RDRS Standing Committee noted the SSAD could better guide users to mitigate against malformed or incomplete requests, particularly when the requests were not submitted with malintent.
[10] In this context, vexatious means requests that are made with the intention of harassing the receiving party, rather than with the intention to make a genuine request for underlying registration data.

7.3.2. Support the ability of a Requestor to submit multiple domain names in a single request.

7.3.3. Route each request individually to the Contracted Party responsible for the disclosure decision (this may require SSAD to split a request into multiple transactions).

7.3.4. Only support requests for current data as described in Recommendation 5.13 (no data about the domain name registration's history).

7.3.5. Notwithstanding the recommendations relating to the management of abusive behavior, MUST have the capacity to handle a reasonable number of requests in alignment with the SLAs established.

7.4. Abusive behavior can ultimately result in suspension or termination of access to the SSAD; however, a graduated penalty scheme should be considered in implementation. There may, however, be certain instances of egregious abuse, such as counterfeiting or stealing credentials, where termination would be immediate.

7.5. As described in 7.1.3, if the SSAD receives a high volume of requests from the same Requestor, the volume alone must not result in a de facto determination of system abuse. The SRT notes that when APIs are added to the SSAD, the availability of production data may better inform what could be considered abusive. Accordingly, the SSAD Standing Committee described in Supplemental Recommendation 12 could, after reviewing relevant data and lessons learned, consider recommending the creation of allow-lists and/or block-lists to account for high volume requestors.

7.6. Before submitting abuse reports, Contracted Parties SHOULD issue a documented warning to the Requestor about their behavior on the first occurrence and retain this warning. If this behavior is repeated, and the Contracted Party files an abuse report, the Contracted Party SHOULD submit clear and compelling evidence demonstrating abusive behavior consistent with 7.1.3.1 - 7.1.3.5 on the part of the Requestor. Such evidence MAY include documented communications, patterns of behavior, or other relevant records. ICANN org or its designee's review of the report will involve a thorough review of the context surrounding the request, consistency with previous actions, and any corroborating information that supports the claim of malicious intent, all subject to ICANN org's or its designee's appreciation of the evidence.

7.6.1. Where reasonably appropriate, Contracted Parties MAY report the abuse immediately upon the first occurrence. For example, in cases of egregious abuse, such as counterfeiting or stealing credentials.

7.7. In considering proportionality under 7.1.3.5, ICANN org or its designee SHOULD consider whether the volume, timing, and manner of submission are reasonably related to legitimate disclosure needs or indicate an intent to disrupt the SSAD or a Contracted Party's ability to process requests within the SLAs referenced in Supplemental Recommendation 4. A high volume of requests, including a large number submitted within a short period of time, should not by itself be considered Abusive where the requests reflect legitimate disclosure needs and are properly prepared. In contrast, intentionally accumulating, coordinating, or submitting requests in a manner intended to overwhelm the SSAD or a Contracted Party could constitute Abusive use.

Recommendation Rationale

Supplemental Recommendation 7 includes important accountability for SSAD users in an effort to protect against potential abuse or misuse of the SSAD. Supplemental Recommendation 7 also provides examples of what constitutes abusive behavior and ensures Contracted Parties have the ability to report potentially abusive behavior. Following reports of abusive behavior, ICANN org would investigate the report and take appropriate action, which could include revoking, suspending, or limiting access to the SSAD.

Supplemental Recommendation 8 [14]: Financial Sustainability

Supplemental Recommendation 8 was formerly numbered as Recommendation 14 under the original EPDP Phase 2 SSAD recommendations.

Overarching Financial Sustainability Principle

8.1. The SRT recommends that the SSAD be designed and operated in a financially sustainable manner. Financial sustainability SHOULD be achieved primarily through a cost-effective and operationally efficient system design rather than through full cost recovery from SSAD requestors.

The funding model MUST NOT impose additional costs on data subjects for the disclosure of registration data. Data subjects MUST NOT be charged a separate fee by the SSAD in connection with the disclosure of their registration data to SSAD requestors.

Fee Structure

8.2. ICANN org SHOULD establish a flexible fee structure for the submission of data disclosure requests through the SSAD. Any fee structure established by ICANN org MUST be consistent with the following principles:

> 8.2.1. Fees SHOULD be set at a level that does not unreasonably discourage legitimate use of the SSAD, taking into account that requestors may submit disclosure requests directly to Contracted Parties without using the SSAD.
>
> 8.2.2. Fees SHOULD reflect and be proportionate to the actual operational costs associated with providing the centralized SSAD service. Fees MUST NOT constitute payment for the underlying registration data or for a decision by a Contracted Party to disclose such data.
>
> 8.2.3. The fee structure MUST provide sufficient flexibility to accommodate different categories of requestors, including through reduced fees, fee waivers, or other appropriate mechanisms. In developing the fee structure, ICANN org SHOULD take into account legal, regulatory, or administrative restrictions that may affect the ability of certain requestors, including governmental entities, to pay fees.

Review of Fee Structure

8.3. The Standing Committee described in Supplemental Recommendation 12 SHOULD review the financial sustainability and fee structure of the SSAD after one (1) year of operation and recommend adjustments, as appropriate. The review SHOULD consider actual operating costs, system utilization, request volumes, the impact of fees on legitimate use of the SSAD, and determine if any adjustments or changes are needed.

Implementation Guidance

System Development

8.4. The SRT expects that the costs for developing, deploying, and operationalizing the system, like the implementation of other adopted policy recommendations, to be initially borne by ICANN org, Contracted Parties, and other parties that may be involved. The SRT expects implementation to consider the operational impact on Contracted Parties and avoid imposing disproportionate costs on Contracted Parties as a result of participation in the SSAD.

Authentication Costs

8.5. Where authentication services are provided by recognized Authentication Providers, the SRT expects Authentication Providers to be responsible for the costs associated with their establishment and operation. This Recommendation does not prescribe whether or how Authentication Providers may recover those costs.

Fee Structure

8.6. The fee structure is to be determined during implementation, but the SRT has suggested that ICANN org MAY consider various options, including nominal fees, a subscription fee, free request allowances, reduced fees, and/or fee waivers, as appropriate.

Recommendation Rationale

The RDRS Standing Committee identified original EPDP Phase 2 Recommendation 14 (now Supplemental Recommendation 8) as requiring a relatively low level of modification. However, during the SRT's review, it became apparent that a number of changes made to other recommendations (particularly those removing universal accreditation in the original EPDP Rec. 1 and 2, the Central Gateway Manager function, and automated disclosure decision-making Recommendation 9) have a direct impact on the assumptions of the Supplemental Recommendation 8 - Financial Sustainability.

As a result, while the core objective of Supplemental Recommendation 8 remains appropriate, the SRT recognizes that certain provisions should be updated to reflect the revised architecture of the SSAD and its expected operational model.

In making these adjustments, the SRT has sought to preserve the original intent of Recommendation 8, ensuring that the SSAD operates in a financially sustainable manner over the long term. The recommended changes are not intended to alter that objective, but rather to recognize that a significantly less complex system should have materially lower implementation and operational costs than those anticipated in the original EPDP Phase 2 Recommendations.

The SRT considers that financial sustainability should be achieved primarily through reducing the overall cost and complexity of the system and improving operational efficiencies, rather than relying on a mandatory per-request fee that may discourage use of the SSAD since requestors may continue to submit requests directly to Contracted Parties without charge. The RDRS SC observed that the RDRS pilot operated successfully without requestor fees. The updated SSAD is not an exclusive access mechanism because requestors retain the ability to submit requests directly to Contracted Parties. If a free alternative exists, a mandatory per-request fee is unlikely to generate sufficient usage to support a sustainable cost-recovery model. Because the development of the centralized system for the disclosure of non-public registration data has been an important priority for many within the ICANN Community, the SRT recommends proceeding with a pragmatic approach that ultimately encourages requestor usage, allows for a consistent user experience, and focuses on operational simplicity.

Supplemental Recommendation 9 [15]: Logging

Supplemental Recommendation 9 was formerly numbered as Recommendation 15 under the original EPDP Phase 2 SSAD recommendations.

9.1. The SRT recommends that the SSAD MUST allow for appropriate logging procedures to facilitate diagnostic monitoring, system troubleshooting, auditing procedures as described in Supplemental Recommendation 10, and reporting requirements as described in Supplemental Recommendation 11. For clarity, the SRT describes logs to mean chronological records of events that occur within the SSAD.

Transaction Logs

9.2. The SSAD MUST log information related to transactions within the SSAD and retain the logs for a period of no less than fifteen (15) months.

9.3. Contracted Parties MUST retain records related to the disposition of SSAD requests for a period of no less than fifteen (15) months.

Authentication Logs

9.4. The SSAD MUST log only the information necessary to track the use of authenticated status, to support operational and compliance audits. For the avoidance of doubt, identity proofing records and supporting documentation used by an Authentication Provider to authenticate a requestor MUST NOT be transmitted to, collected by, or retained by the SSAD.

Implementation Guidance

9.5. The SRT is providing the below non-exhaustive list of information it expects the SSAD to log:

9.5.1. Logging related to all SSAD requests:

9.5.1.1. Requestor

9.5.1.2. Domain name(s)

9.5.1.3. Date and time stamps for the request (creation and disposition)

9.5.1.4. Request type

9.5.1.5. Priority Level

9.5.1.6. Data elements requested

9.5.1.7. Jurisdiction where the nonpublic registration data will be processed

9.5.1.8. Contracted Party in receipt of request

9.5.1.9. Results of processing the query, including change of state and timestamps for each state (e.g., received, pending, in-process, denied, approved, approved with changes)

9.5.1.10. Rates of disclosure and non-disclosure

9.5.1.11. If the SSAD request is approved, data elements provided.

9.5.1.12. If the SSAD request is partially approved, data elements disclosed plus reason(s) for denying the remainder of the request

9.5.1.13. If the SSAD request is denied, the rationale for the denial.

9.5.2. Logging related to Authenticated Requestors:

9.5.2.1. Authentication event information (use of authenticated status, Authentication Provider, validation result and timestamps)

9.5.2.2. Authentication transaction information (e.g. requestor community, and receiving Contracted Party)

9.5.2.3. Operational metrics (e.g. authenticated request volumes, Authentication Provider usage, validation failures)

9.5.2.4. security and audit events (e.g. authentication processing errors).

9.6. If logged data contains personal information, the personal information MUST remain confidential for reporting purposes and appropriate safeguards need to be put into place.

9.7. Logs MAY be disclosed in certain instances, including, for example,

9.7.1. Claims of misuse, where logs may be requested for examination by ICANN org or its designee;

9.7.2. Audits, where logs may be requested for examination by ICANN org or the auditing body.

9.7.3. Instances when logs are mandated as a result of due process, including relevant enforcement and regulatory authorities

9.7.4. Technical operations, in order to ensure proper running of the system.

9.8. Where the SSAD system is required to log data elements pertaining to a disclosure request, the SRT specifies this to mean the SSAD system must record only the category of data (e.g., "Name") and not the underlying data itself (e.g., "John Doe".)

9.9. Regarding 9.3, the SRT expects Contracted Parties to maintain logs of acknowledgements and responses to SSAD requests in accordance with standard business recordation practices, so that they are available to be produced as needed including, but not limited to, for audit purposes by ICANN org.

9.10. The retention period for records required to be retained pursuant to 9.3 should begin when an SSAD request is closed.

9.11. In cases where a third party provider receives or responds to disclosure requests submitted through the SSAD, Contracted Parties MUST ensure they or their third-party provider retain records in accordance with 9.3.

Recommendation Rationale

Supplemental Recommendation 9 ensures that important SSAD-related activities are appropriately logged and retained for the purposes of system learning, gathering data/statistics to improve the SSAD over time, auditing, and reporting purposes.

Supplemental Recommendation 10 [16]: Auditing

Supplemental Recommendation 10 was formerly numbered as Recommendation 16 under the original EPDP Phase 2 SSAD recommendations.

Audits of the Authentication Providers

10.1. The SRT recommends that ICANN org or its designee MUST periodically audit recognized Authentication Providers for compliance with the requirements established pursuant to Supplemental Recommendation 1.

10.2. 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.

10.3. Should the Authentication Provider be found in breach of the requirements established pursuant to Supplemental Recommendation 1, it will be given an opportunity to cure the breach; however, in cases of repeated non-compliance or audit failure, ICANN org or its designee MAY

cancel or terminate the Authentication Provider's status as a recognized Authentication Provider for the SSAD.

10.4. Any audit of an Authentication Provider MUST be tailored for the purpose of assessing compliance with the policy requirements as outlined and established by ICANN org or its designee (per Supplemental Recommendation 1 of this policy), 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.

10.5. As part of such audits, the Authentication Provider MUST provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the policy requirements as outlined and established by ICANN org or its designee (per Supplemental Recommendation 1 of this policy).

Audits of the SSAD

10.6. ICANN org or its designee is expected to conduct periodic audits of the system assessing the technical functioning of the SSAD system and MAY incorporate changes, if needed, based on the results of the audits.

Reporting of Audits

10.7. ICANN org SHOULD establish regular public reporting on the audits described in 10.3 and 10.6, to confirm audits are occurring and to publish high-level results of the audits.

Auditing of Requestors

10.8. ICANN org or its designee MUST review and investigate verified complaints concerning a Requestor's compliance with the SSAD Terms and Conditions, Terms of Use, or Acceptable Use Policy, including allegations of abusive use of the SSAD, in accordance with Supplemental Recommendations 6 and 7.

For purposes of this Recommendation, auditing of Requestors means investigation of a verified complaint regarding a Requestor's compliance with applicable terms or verified complaints regarding a Requestor's alleged abusive use of the SSAD. Complaint-based auditing of Requestors is distinct from the periodic auditing of Authentication Providers and the SSAD, described in 10.1 and 10.6, respectively. The SRT is not recommending periodic or random audits of Requestors. Instead, the complaint-based auditing described above is intended to support Requestor accountability by enabling ICANN org or its designee to assess reported non-compliance with applicable SSAD requirements or alleged abusive use of the SSAD and, where appropriate, take action in accordance with Supplemental Recommendations 6 and 7.

Implementation Guidance

10.9. For the periodic audits described in 10.3 and 10.6, the SRT suggests that these audits could occur on an annual basis, but notes that flexibility on time periods may be necessary. Additionally, the SRT notes that audits described in 10.3 and 10.6 SHOULD also occur upon complaint.

Recommendation Rationale

Supplemental Recommendation 10 ensures appropriate auditing is in place. Supplemental Recommendation 10 provides specifically for the auditing of Authentication Providers. For clarity, auditing (upon complaint) of requestors is provided for in Supplemental Recommendations 6 and 7. Periodic auditing of Contracted Parties is provided for in ICANN contracts (Registry Agreement and Registrar Accreditation Agreement) and auditing upon complaint is provided for in Supplemental Recommendation 5. Periodic auditing of Authenticated Users is covered in Supplemental Recommendation 1.

Supplemental Recommendation 11 [17]: Reporting

Supplemental Recommendation 11 was formerly numbered as Recommendation 17 under the original EPDP Phase 2 SSAD recommendations.

11.1. The SRT recommends that ICANN org MUST establish regular public reporting on the use and functioning of the SSAD. For the avoidance of doubt, this recommendation does not intend to prevent ICANN org from conducting additional non-public reporting to SSAD users.

11.2. No earlier than 3 months and no later than 9 months after the operationalization of SSAD, ICANN org MUST publish an SSAD Status Report or dashboard, and continue to do so on a quarterly basis.

Implementation Guidance

11.3 The SRT expects quarterly reports to include at a minimum:

- Number of disclosure requests received; including requests for the underlying data for domains using privacy or proxy services received, where the Contracted Party accepts such requests;
- Average response times to the disclosure requests, categorized by request type;
- Number of requests categorized by third-party purposes / justifications (as identified in Supplemental Recommendation 2);
- Number of disclosure requests approved, denied, ICANN review, or additional information needed;
- Number of denied disclosure requests, categorized by denial reason;
- Number of LEA disclosure requests by country, by economy and by category, where noted by requestor;
- Number of requests classified by the requestor as Urgent;
- Number of requests classified by the requestor as Standard;
- Number of requests reclassified by the Contracted Party (in other words, requests marked as Urgent that are reclassified by the Contracted Party as Standard Requests or are reclassified by the Contracted Party from Standard to Urgent);
- Information about financial sustainability of SSAD;
- Technical or system difficulties, i.e., incident reporting;
- Operational and system enhancements.

The SRT expects any updates to the above non-exhaustive list, e.g., additions or removals, to be done in conjunction with the SSAD Standing Committee as described in Supplemental Recommendation 12. Any updates to the list would be considered implementation, not policy development.

11.4. The SRT recommends that further consideration is given during implementation to:

- The frequency of public reporting – public reporting on a quarterly basis would be considered reasonable. Note: during the RDRS Pilot, ICANN org reported on the RDRS on a monthly basis, but the RDRS Standing Committee, in line with Rec. 11.3, noted detailed quarterly reporting would be reasonable;
- Data to be reported on, which is expected to include information such as:
    a. number of disclosure requests;
    b. disclosure requests per category of Requestors;
    c. disclosure requests per Requestor (for legal entities);
    d. disclosure requests granted / denied, and;
    e. response times.

  Please note that this is a non-exhaustive list.
- Mechanism for public reporting – consider the possibility of a publicly available dashboard instead of or in addition to reports that are posted;
- Needs for possible confidentiality in certain cases such as information about natural persons and LEA requests. Aggregate data or pseudonymization could be considered to address possible confidentiality concerns.

Recommendation Rationale

Supplemental Recommendation 11 endeavors to ensure that important data points are transparently reported and provided to the ICANN Community, and in particular, the SSAD Standing Committee, who will recommend improvements to the SSAD. Supplemental Recommendation 11 ensures that the SSAD Standing Committee has the data it needs to assess and recommend important improvements to the SSAD.

Supplemental Recommendation 12 [18]: SSAD Standing Committee

Supplemental Recommendation 12 was formerly numbered as Recommendation 18 under the original EPDP Phase 2 SSAD recommendations.

Establishment and Purpose

12.1.1. The SRT recommends that the GNSO Council MUST establish a Standing Committee to review the operation of the SSAD following its implementation. The Standing Committee will be responsible for reviewing the publicly reported SSAD metrics[11] (see Supplemental Recommendation 11) to identify operational issues and potential implementation improvements.

12.1.2. For purposes of this Recommendation, “operational issues” are issues concerning the implementation, functionality, performance, or use of the SSAD that arise through SSAD

[11] Supplemental Recommendation 11 recommends ICANN org to provide SSAD metrics on a quarterly basis.

operations. For example, the Standing Committee may review SSAD metrics (See Supplemental Recommendation 11) or community feedback and identify recurring difficulties with request submission or processing and recommend implementation-level changes, such as improvements to forms, user messaging, reporting, or metrics.

12.1.3. The Standing Committee is an advisory body and does not have the authority to create, amend, or interpret Consensus Policy or to direct ICANN org. Where the Standing Committee identifies an issue that would require a change to existing Consensus Policy, the Standing Committee MAY document the issue and refer[12] it to the GNSO Council for further consideration through the appropriate GNSO process.

Charter

12.2. The GNSO Council MUST establish a Charter for the Standing Committee consistent with the following principles:

12.2.1. **Composition:** The Standing Committee shall include representation from the ALAC, BC, GAC, IPC, ISPCP, NCSG, RrSG, RySG and SSAC, with at least one member and one alternate from each group, and a GNSO Council liaison. The Charter may provide for ICANN org liaisons and additional subject matter experts to participate as appropriate. The Standing Committee will appoint the Chair, and the Chair is not required to be a member of a GNSO Stakeholder Group or Constituency.

12.2.2. **Scope**

12.2.2.1. As noted in Section 12.1.1, the Standing Committee will be responsible for reviewing publicly reported SSAD metrics (See Supplemental Recommendation 11) and community feedback, where applicable, concerning the operation of the SSAD to identify operational issues and potential implementation improvements.

12.2.2.2. Operational issues may be raised by a Standing Committee member, ICANN org or referred to the Standing Committee by the GNSO Council. The Standing Committee may communicate identified operational issues and recommended improvements to ICANN org and/or the GNSO Council, as appropriate.

12.2.2.3. For the avoidance of doubt, nothing in this recommendation limits ICANN org's ability to make operational, administrative, technical, security, maintenance, or other implementation-level changes to the SSAD consistent with applicable Consensus Policy without prior consultation with or approval by the Standing Committee or GNSO Council.

12.2.2.4. The Standing Committee is expected to work with ICANN org to consider operational and implementation changes to the SSAD. Where the Standing Committee and ICANN org agree, the proposed changes need NOT be referred to or approved by the GNSO Council; however, the GNSO Council

[12] For example, the RDRS Standing Committee made recommendations to the GNSO Council, where it identified areas where the Council could consider further policy work; however, the RDRS Standing Committee's recommendations were not policy recommendations. The SRT envisions the SSAD Standing Committee to function in a similar way.

liaison is expected to keep the GNSO Council informed of the Standing Committee's work.

12.2.3. Consensus

12.2.3.1. The Standing Committee MAY submit recommendations to the GNSO Council where it identifies (i) an area for further policy work or (ii) a proposed operational change that would require significant resources. When submitting such recommendations, Section 3.6 of the GNSO Working Group Guidelines SHOULD be used as guidance, rather than as a strict mandate, for assessing the level of agreement within the Standing Committee. Where there is disagreement, the Standing Committee MUST document the different views or positions and allow groups to submit minority statements.

12.2.4. Similar to the Supplemental Recommendations Team, the SRT recommends that the Standing Committee MUST consider the needs of Contracted Parties, requestors, and data subjects when proposing updates to the SSAD.

12.2.5. Review and Disbanding

On an annual basis, the GNSO Council SHOULD evaluate whether the Standing Committee's charter, composition, and responsibilities remain appropriate and fit for purpose.

The Standing Committee may recommend that it be disbanded by an affirmative vote of a simple majority of the represented groups. Any such recommendation is subject to approval by the GNSO Council.

Implementation Guidance

12.3. Throughout these Supplemental Recommendations, the SRT has identified specific matters for which the Standing Committee has a review, consultation, monitoring, or advisory role. These include, for example, matters referenced in Recommendations 1.5, 1.7, 2.9, the rationale to Supplemental Recommendation 4, 7.5, 11.3, and 8.3. In developing the Standing Committee's Charter, the GNSO Council SHOULD take these references into account. The list is illustrative and not exhaustive and is not intended to limit the Standing Committee's ability to consider other operational issues consistent with the scope of Supplemental Recommendation 12. For clarity, these cross-references do not transfer the underlying policy obligations in those Recommendations to the Standing Committee. Rather, they identify areas in which the Standing Committee may have a review or advisory role.

Recommendation Rationale

As the SSAD is a new system, the SRT notes it will be critical to review and evaluate the learnings from the SSAD and suggest improvements, where needed. The SRT and RDRS Standing Committee noted the productive, constructive, and collegial way in which the RDRS Standing Committee worked with ICANN org to make improvements to the RDRS based on

lessons learned. The SRT suggests continuing in a similar manner will enhance the ultimate viability and utility of the SSAD and benefit all SSAD users.

High-Level Summary of Impact Assessment

As per its assignment, the SRT is expected to include “a statement on the WG discussion concerning impact of the proposed recommendations, which could consider areas such as economic, competition, operations, privacy and other rights, scalability and feasibility.” This section is also expected to address the expected impact, if any, on human rights.

The following impact assessments were grouped into these categories:

- Human Rights Impact Assessment
- Data Privacy Considerations
- Global Public Interest Checklist
- Potential Impact on existing Consensus Policies

Once the SRT Preliminary Recommendations became more stable, the SRT conducted its impact assessments as summarized below and accessible HERE.

The Impact Assessment is intended to provide a structured view of the potential human rights, data protection, public interest, and Consensus Policy implications of the Supplemental Recommendations.

The SRT approach was to identify the most material potential impacts and consider the safeguards and mitigation built into the proposed policy framework. At a high level, the work reflects an effort to balance legitimate access to non-public registration data with appropriate protections for data subjects, while also considering accountability, operational feasibility, public interest, and consistency with existing Consensus Policies.

Annex 1 – Original Working Draft Recommendation Order

The updated Supplemental Recommendation order reflects the GNSO Council's agreement to merge overlapping and related text and remove text that was no longer fit for purpose. Specifically, the new order of the Supplemental Recommendations reflects the following:

Original EPDP Phase 2 Recommendation	Supplemental Recommendation
1: Accreditation	1: Authentication
2: Accreditation of Governmental Entities Recommendation	Relevant text merged with SupRec2: Criteria and Content of Requests
3: Criteria and Content of Requests	2: Criteria and Content of Requests
4: Acknowledgement of Receipt and Relay of the Disclosure Request	3: Acknowledgement of Receipt and Relay of the Disclosure Request
5: Response Requirements	Relevant text merged with SupRec5: Contracted Party Disclosure Decision
6: Priority Levels	4: Request Types and Service Level Agreements
7: Requestor Purpose	Relevant text merged with SupRec2: Criteria and Content of Requests
8: Contracted Party Authorization	5: Contracted Party Disclosure Decision
9: Automation of SSAD Processing	Relevant text merged with SupRec3: Acknowledgement of Receipt and Relay of the Disclosure Request
10: Determining Variable SLAs for Response Times for SSAD	4: Request Types and Service Level Agreements
11: SSAD Terms and Conditions	6: SSAD Agreements and Policies
12: Disclosure Requirement	Relevant text merged with SupRec 5: Contracted Party Disclosure Decision
13: Query Policy	7: Query Abuse Policy
14: Financial Sustainability	8: Financial Sustainability

15: Logging	9: Logging
16: Auditing	10: Auditing
17: Reporting	11: Reporting
18: Review of implementation of policy recommendations concerning SSAD using a GNSO Standing Committee	12: SSAD Standing Committee

Annex 2 – SSAD Supplemental Recommendations Team Assignment Form

Subject	Non-Adopted SSAD Recommendations
Background	On 29 October 2020 the GNSO Council submitted to the ICANN Board its Recommendations Report on the Expedited Policy Development Process (EPDP) Temporary Specification for gTLD Registration Data Phase 2. On 25 March 2021, the ICANN Board directed ICANN org to perform an Operational Design Phase (ODP) on the EPDP Temporary Specification for gTLD Registration Data Phase 2 and the System for Standardized Access/ Disclosure (SSAD) to Nonpublic generic Top-Level Domain Registration Data (SSAD Recommendation 1-18). On 25 January 2022, ICANN org delivered the Operational Design Assessment (ODA), the main output of the ODP. The GNSO Council subsequently tasked the EPDP Phase 2 Small Team (Small Team) with assessing the ODA. At the GNSO Council's request, the Board paused its consideration of the SSAD recommendations while work on a "proof of concept" was being conducted. This "proof of concept" eventually became the Registration Data Request Service (RDRS). The RDRS was used to collect data about system usage, which was to be used to help inform future discussions between the GNSO Council and the ICANN Board on the pending SSAD Recommendations 1–18. Data collected from the RDRS was assessed by the RDRS Standing Committee. The Standing Committee's report provided 6 recommendations, including a recommendation for the Board to "consider the 18 recommendations together as one package. The SC further recommends that when the GNSO Council and ICANN Board engage in a dialogue, the Council should recommend that the ICANN board reject the SSAD recommendations (as a package) and send them back to the GNSO Council for further action and Supplemental Recommendation." The Standing Committee recommended non-adopting all 18 SSAD recommendations as they were developed and adopted by the GNSO Council as a comprehensive and interdependent package. Furthermore, the Standing Committee provided detailed suggestions on how to keep or modify each of the 18 SSAD recommendations. On 12 March 2026, the Board passed a resolution, not adopting the pending SSAD recommendations. In its resolution, the Board noted after reviewing input from the community, engaging with the Standing Committee, and consulting the GNSO Council on the SSAD policy recommendations, that the SSAD Recommendations in the EPDP Phase 2 Final Report were not in the best interests of the ICANN

	community or ICANN. The Board's non-adoption of the pending SSAD recommendations in order to trigger the Supplemental Recommendation process is outlined in Annex A, Section 9 of the ICANN Bylaws. 1 As noted in the discussion on 12 February 2026 between the Board and GNSO Council, non-adoption was recommended by the Standing Committee, and is an opportunity for the GNSO Council to issue Supplemental Recommendations. For the avoidance of doubt, non-adoption should not be interpreted as an opportunity to relitigate carefully drafted compromises, viewed as the SSAD recommendations being discarded, or a signal that the Board will not adopt Supplemental SSAD Recommendations. The GNSO Council has determined that an SSAD Supplemental Recommendations Team consisting of Councilors in combination with additional ICANN Community members is the appropriate mechanism to carefully analyze Supplemental Recommendations, consider Board concerns and Standing Committee recommendations, and, where deemed appropriate, recommend proposed modifications to the non-adopted recommendations for the GNSO Council's consideration.
Assignment	**Task**: The SSAD Supplemental Recommendations Team is expected to address the following assignment: 1) Provide Supplemental Recommendations* on all SSAD recommendations 2) Advise the GNSO Council on any specific questions or issues to raise during meetings with the ICANN Board concerning SSAD; 3) Propose modifications to SSAD recommendations based on the recommendation rationale provided in the Standing Committee's Final Findings Report. *In drafting proposed Supplemental Recommendations, the SSAD Supplemental Recommendations team is expected to consider: - the potential impact of any recommendations on the Global Public Interest (see example checklist); - the potential impact of any recommendations on human rights (see HRIA tool and Human Rights Framework of Interpretation HR-FOI); - the potential impact on existing Consensus Policies. The SSAD Supplemental Recommendations Team is expected to refer back to the GNSO Council if there is strong support in the group for the view that a particular proposed outcome may be out of scope of the Assignment, (e.g., developing new policy versus modifications rooted in foundational documents).This is not meant to restrict a Councilor's or Councilors' ability to independently raise issues to the full Council.

	In addition to the above, the Board has requested the Council to consider the following four elements in its development of Supplemental Recommendations: 1. Mandatory registrar participation in mechanisms for requesting 2 gTLD nonpublic registration data, which align with the presumption that consensus policies are binding on all contracted parties. 2. Confirmation of how the mechanism can be used to make and respond to requests for gTLD nonpublic registration data for underlying affiliated privacy/proxy domains. 3. Inclusion of service level agreements that require registrars to provide substantive responses to disclosure requests on an agreed timeline for urgent requests that are authenticated, as originally envisioned in the SSAD recommendations. 4. An authentication mechanism for law enforcement authorities and a phased approach for federated authentication for other user groups to facilitate urgent request responses, as originally envisioned in the SSAD recommendation. The Board noted that these four elements will help produce a long-term solution for requesting access to gTLD nonpublic registration data. The SSAD Supplemental Recommendations Team is expected to consider whether these four elements can be addressed via Supplemental Recommendation. If the conclusion is that any of them cannot be so addressed through this process, the SSAD Supplemental Recommendations Team may choose to make a recommendation to Council for how they may be addressed through some other mechanism. The SSAD Supplemental Recommendations Team is advised to take into account the: ● EPDP on the Temporary Specification for gTLD Registration Data Phase 2 Final Report ● RDRS Standing Committee Final Findings Report and the recommendations therein; ● GAC Advice from ICANN64, ICANN70, and ICANN79; ● SAC 118: SSAC Comments on Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A; ● SSAD Operational Design Assessment ● RDRS Policy Alignment Analysis and Public Comment Summary; and ● Timeline for Urgent Requests and Public Comment Summary Please see the “Documents” section below for additional supporting information. The SSAD Supplemental Recommendations Team will be asked to deliver a report to the GNSO Council containing Supplemental

	Recommendations, the rationale for the Supplemental Recommendations, and any additional information deemed necessary for GNSO Council consideration. The final decision on the Supplemental Recommendations rests with the GNSO Council.
Timing	The SSAD Supplemental Recommendations Team shall commence its 3 work after the Board's non-adoption. The Board non-adopted the recommendations at its meeting on 12 March 2026. The SSAD Supplemental Recommendations Team is expected to deliver proposed Supplemental Recommendations, the rationale for the Supplemental Recommendations, and any additional information deemed necessary for GNSO Council consideration by **February 2027**.
Members	**Membership**: The SSAD Supplemental Recommendations Team shall be open to any interested and committed GNSO Councilor. Additionally, the SSAD Supplemental Recommendations Team can invite up to: ● Two (2) members of the Registries Stakeholder Group (RySG); ● Two (2) members of the Registrar Stakeholder Group (RrSG); ● One (1) member of the Business Constituency; ● One (1) member of the Intellectual Property Constituency; ● One (1) member of the Internet Service Providers and Connectivity Providers Constituency; ● Three (3) members of the Non-commercial Stakeholder Group; ● One (1) member and one (1) alternate from the At-Large Advisory Committee ● One (1) member and one (1) alternate from the Governmental Advisory Committee; and ● One (1) member and one (1) alternate from the Security and Stability Advisory Committee The SSAD Supplemental Recommendations Team may be assigned the following liaisons: ● At least one (1) member of the ICANN Board ● At least one (1) member of ICANN org staff (focusing on implementation) The SSAD Supplemental Recommendations Team is expected to be familiar, or familiarize themselves, with the SSAD recommendations (Recs. 1-18) in the EPDP (RegData) Phase 2 Final Report and the RDRS Standing Committee Final Findings Report. **Leadership**: A lead for the SSAD Supplemental Recommendations Team will be determined once the SSAD Supplemental Recommendations Team has been established. The role of the Lead of the SSAD Supplemental Recommendations Team is to lead

	meetings and provide updates to the full GNSO Council. If and when the Lead is to discuss the topic outside of the Council context, the GNSO Council shall agree on talking points. **ICANN org liaison(s)**: ICANN org's GDS function is invited and encouraged to assign at least one liaison to support the SSAD Supplemental Recommendations Team. **ICANN Board liaison(s)**: The ICANN Board is invited and encouraged to assign at least one liaison to support the SSAD Supplemental Recommendations Team. The SSAD Supplemental Recommendations Team's objective is to present the GNSO Council with recommendations that have the full consensus of the SSAD Supplemental Recommendations Team. Should this not be possible, the Lead is expected to assess the level of consensus achieved (as per the GNSO Working Group Guidelines) and communicate this to the GNSO Council together with the different views expressed.
Documents	• EPDP on the Temporary Specification for gTLD Registration Data Phase 2 Final Report: EPDP on the Temporary Specification for gTLD Registration Data Phase 2 Final Report. • Registration Data Request Service Standing Committee Council Report: https://gnso.icann.org/sites/default/files/policy/2025/draft/rdrs-sc-findings-report-10nov25-en.pdf • RDRS Policy Alignment Analysis: https://itp.cdn.icann.org/en/files/registration-data-request-service-rdrs/registration-data-request-service-policy-alignment-analysis-30-10-2025-en.pdf • RDRS Policy Alignment Analysis Public Comment Summary Report: https://itp.cdn.icann.org/en/files/registration-data-request-service-rdrs/summary-report-rdrs-policy-alignment-analysis-20-01-2026-en.pdf • Timeline for Urgent Requests and Public Comment Summary: https://itp.cdn.icann.org/en/files/new-generic-top-level-domain-gtld-program/summary-report-timeline-ur-lawful-disclosure-non public-registration-data-14-01-2026-en.pdf • 02 March 2026 Correspondence - GNSO Council Dialogue with ICANN Board re: SSAD Recommendations: https://itp.cdn.icann.org/en/files/correspondence/payne-to-sinha-0 2-03-2026-en.pdf. • 18 March 2026 Correspondence - GNSO Expedited Policy Development Process (EPDP) Phase 2 Final Report and the System for Standardized Access/Disclosure (SSAD) Policy Recommendations: https://itp.cdn.icann.org/en/files/correspondence/sinha-to-payne-18-03-2026-en.pdf

	• 12 March 2026 ICANN Board Resolution: https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-regular-meeting-of-the-icann-board-12-03-2026-en#section2.a • ICANN64 GAC Advice: https://gac.icann.org/contentMigrated/icann64-kobe-communique • ICANN70 GAC Advice: https://gac.icann.org/contentMigrated/icann70-gac-communique?language_id=1 • ICANN79 GAC Advice: https://gac.icann.org/contentMigrated/icann79-san-juan-communique?language_id=1 • SAC 118: SSAC Comments on Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A: https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-118-en.pdf • SSAD Operational Design Assessment: https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf
Documentation of Work	• A wiki page will be created to capture at a minimum, membership, background document and new documents generated by the SSAD Supplemental Recommendations Team, and meeting recordings. • Unless a specific meeting might benefit from an unrecorded dialogue, all meetings will be recorded. In this exceptional instance, transparency will be accounted for in some other fashion (e.g., notes, readout, report, etc.). • A mailing list will be created for this SSAD Supplemental Recommendations Team and will be publicly archived on the Wiki. Observers may request to be added to the mailing list on a read-only basis. • Observers may attend meetings live; however, observers will have no speaking or chat privileges.
Next Steps	1. Following GNSO Council approval / non-objection, SSAD Supplemental Recommendations Team to commence work on providing Supplemental Recommendations to the SSAD recommendations 2. SSAD Supplemental Recommendations Team to reach out to GNSO SG/Cs and interested ACs to request identification of SMEs to assist the SSAD Supplemental Recommendations Team. 3. SSAD Supplemental Recommendations Team to develop a 6 high-level timeline for next steps to allow for advance scheduling and check-ins with GNSO Council.