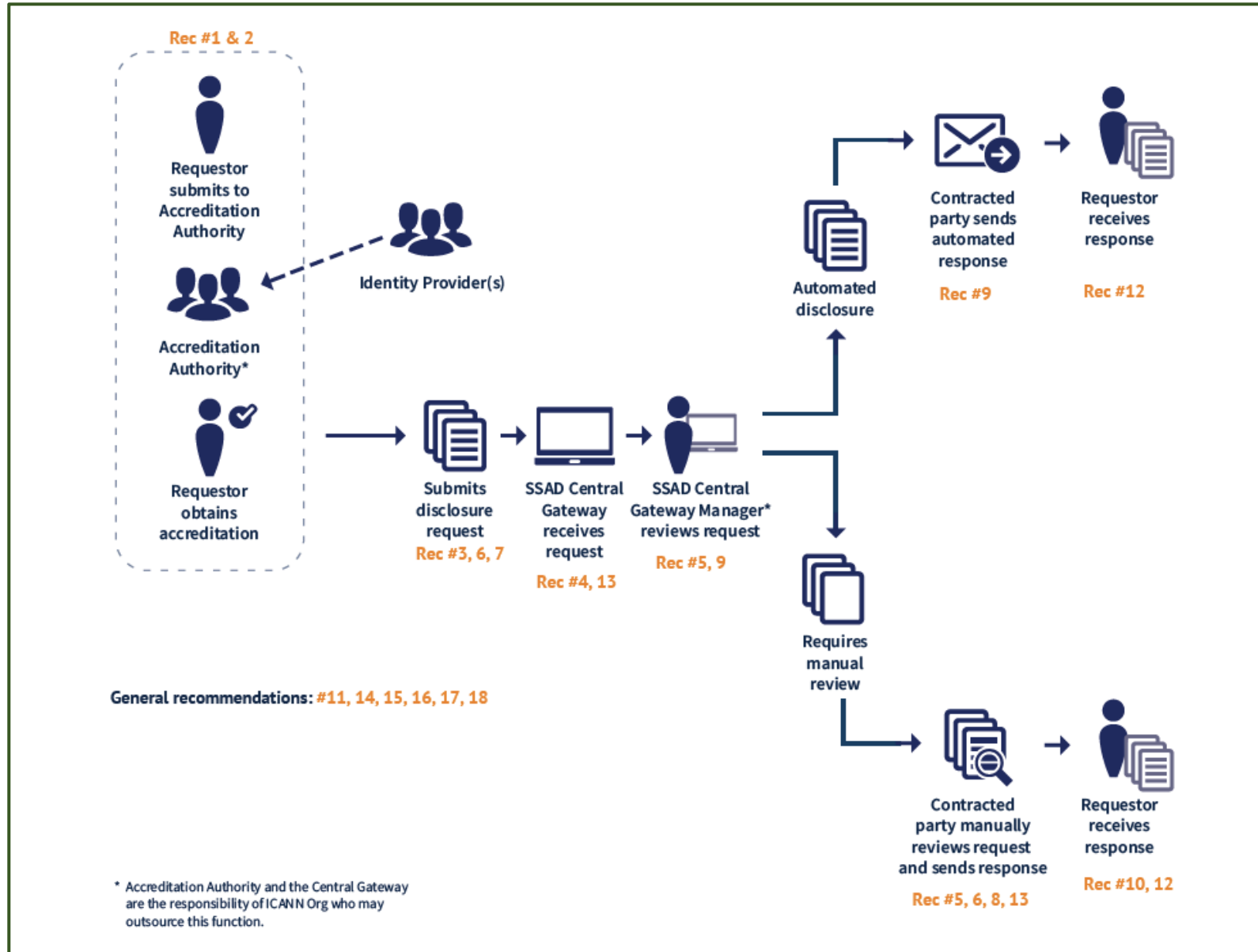


GNSO Council – EPDP Phase 2 Final Report Webinar



SSAD Related Recommendations (#1 - #18)

SSAD High Level Overview

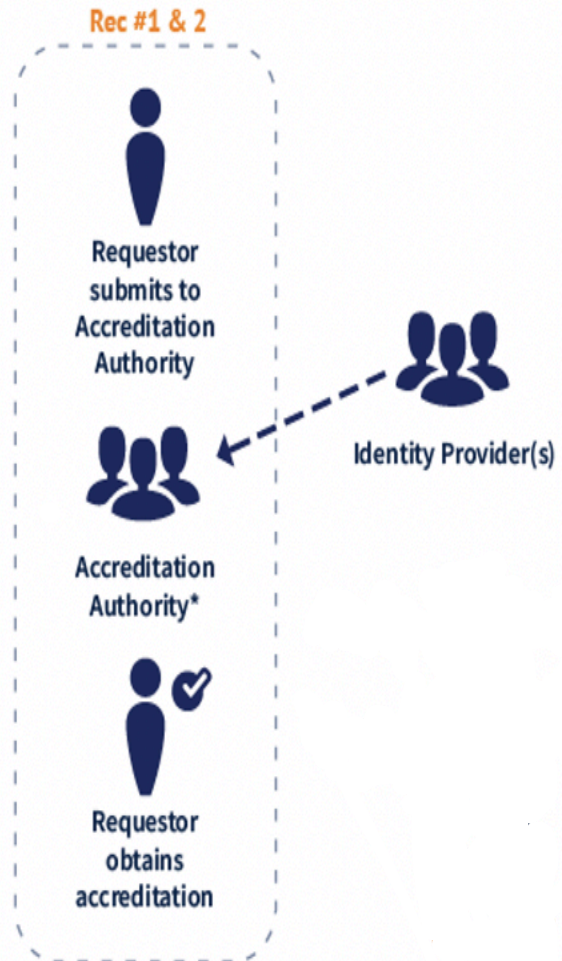


Accreditation High-Level Overview (Rec. 1)



- Accreditation Authority (ICANN or its assignee) to set accreditation policy. Policy recs outline main principles of such policy.
- SSAD to only accept disclosure requests from accredited organizations or individuals.
- Both legal persons and/or individuals are eligible for accreditation
- Accreditation Authority may, but is not obligated to, work with external or third-party Identity Providers that could serve as clearinghouses to verify identity and authorization information associated with requestors.
- Rec. 1 details specific requirements of the Accreditation Authority, including:
 - Verifying and validating identity of requestor
 - Develop a code of conduct, privacy policy, baseline application procedure, dispute resolution/complaints procedure, renewal procedure
 - Auditing requirements – must be subject to regular audits
 - Reporting requirements – must report publicly on application metrics
- Org to use its experience with registrar accreditation to put forward a proposal for the verification of identity during implementation

Accreditation High-Level Overview – Identity Providers



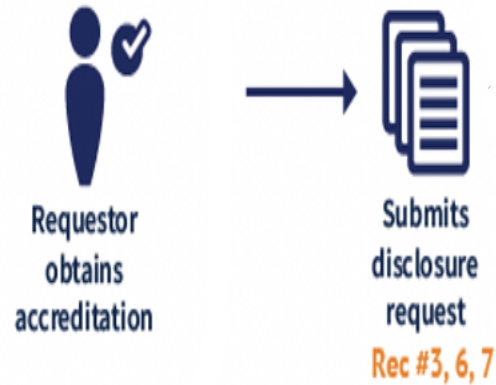
- Identity Providers may be:
 - ICANN itself as the Accreditation Authority
 - Third party assignee(s) of the Accreditation Authority
- Identity Providers are responsible for:
 - 1) Verifying the identity of a Requestor and managing any credentials associated with identity verification
 - 2) Verifying and managing Signed Assertions associated with a unique requestor. Signed Assertions are data objects associated to a specific identity, such as a user having rights in a specific trademark(s) or a user's identity as a professional cyber security firm.
- Accreditation Authority may de-accredit an identity provider

Accreditation of Gov't Entities High-Level Overview (Rec. 2)



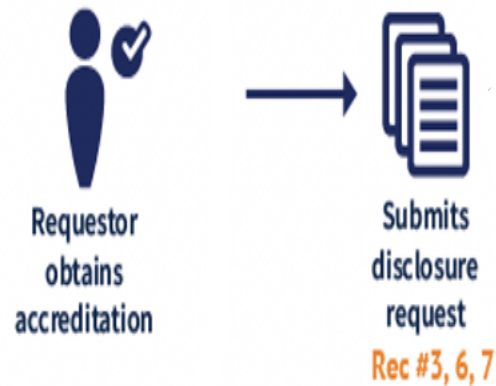
- Per Rec. 2, eligible entities that may be accredited by their country's/territory's government body or its authorized body (such as an IGO) include:
 - Civil and criminal law enforcement authorities
 - Data protection and regulatory authorities
 - Judicial authorities
 - Consumer rights organizations 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)
- Eligibility for accreditation is determined by a country/territory-designated Accreditation Authority.
- Accreditation requirements for gov't entities must mirror requirements for legal persons and individuals described in Rec. 1 and must be listed and made available to gov't accreditation authorities

Disclosure Requests (Recs. 3, 6, 7)



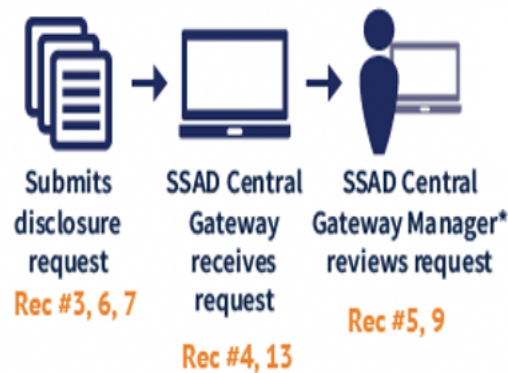
- SSAD must allow for the standardized submission of disclosure requests
- SSAD requests must include, at a minimum:
 - Domain name
 - Info on identity of requestor
 - Legal rights of requestor
 - Affirmation that the request is made in good faith and that data received (if any) will be processed lawfully and only in accordance with the purposes specified
 - Requested data elements
 - Request type (priority level, confidential, urgent)
- Upon receipt, Central Gateway Manager performs a completeness check (are all required fields filled out, no substantive check, if not complete, it will not be possible for requestor to submit)
- Requestors must submit disclosure requests for specific purposes (non-exhaustive list is provided in Rec. 7).
- A requestor's assertion of any specific purpose does not guarantee access/disclosure.

Disclosure Requests (Recs. 3, 6, 7)



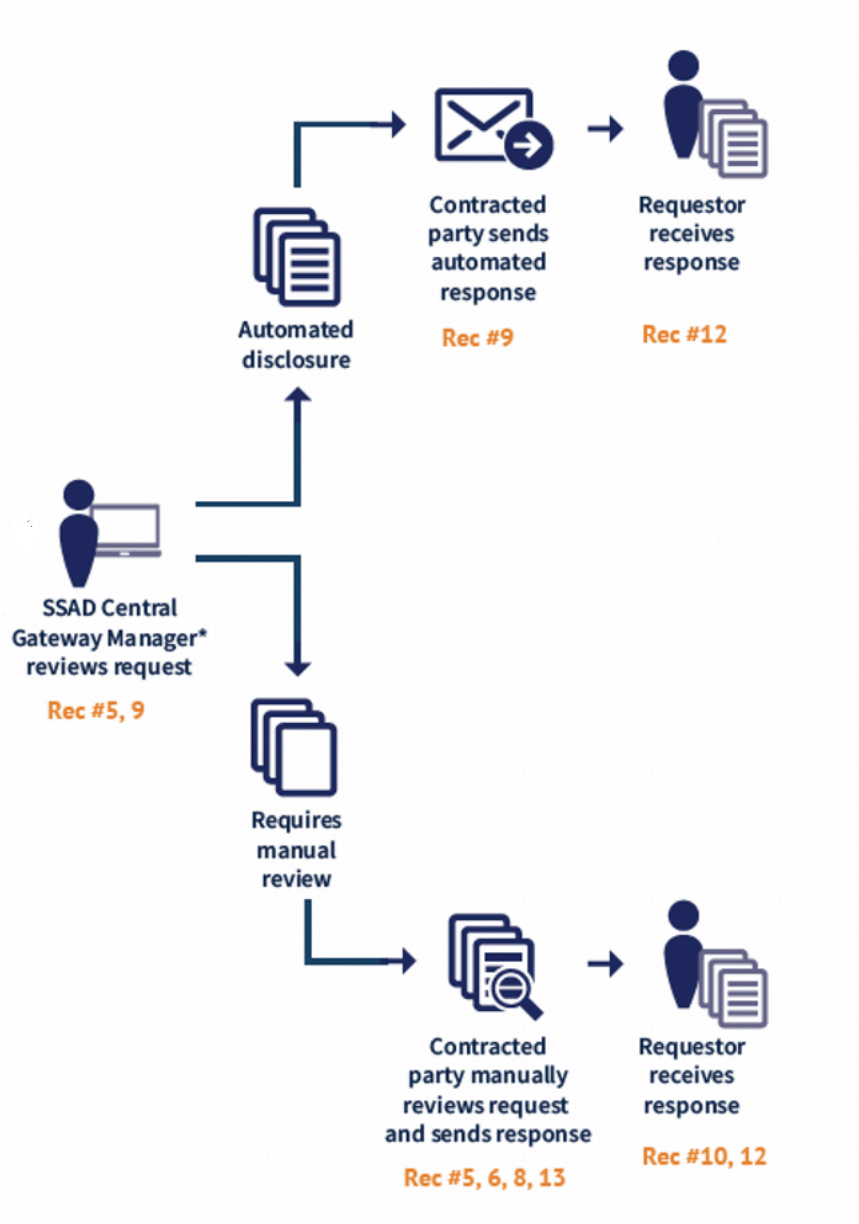
- SSAD must allow requestor to choose from three priority levels:
 - **Priority 1** - Urgent Requests - The criteria to determine urgent requests is limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation.
 - **Priority 2** – ICANN administrative proceedings (Providers verifying a UDRP/URS request).
 - **Priority 3** – all other requests. Note: SSAD must allow requestors to indicate that the disclosure request concerns a consumer protection issue (phishing, malware or fraud), and CPs may prioritize these requests.
- CPs may reassign the priority level – any reassignment will be communicated to requestor
- Abuse of urgent request designations may result in suspension from submitting urgent requests via SSAD

SSAD's receipt of requests (Recs. 4 + 13)



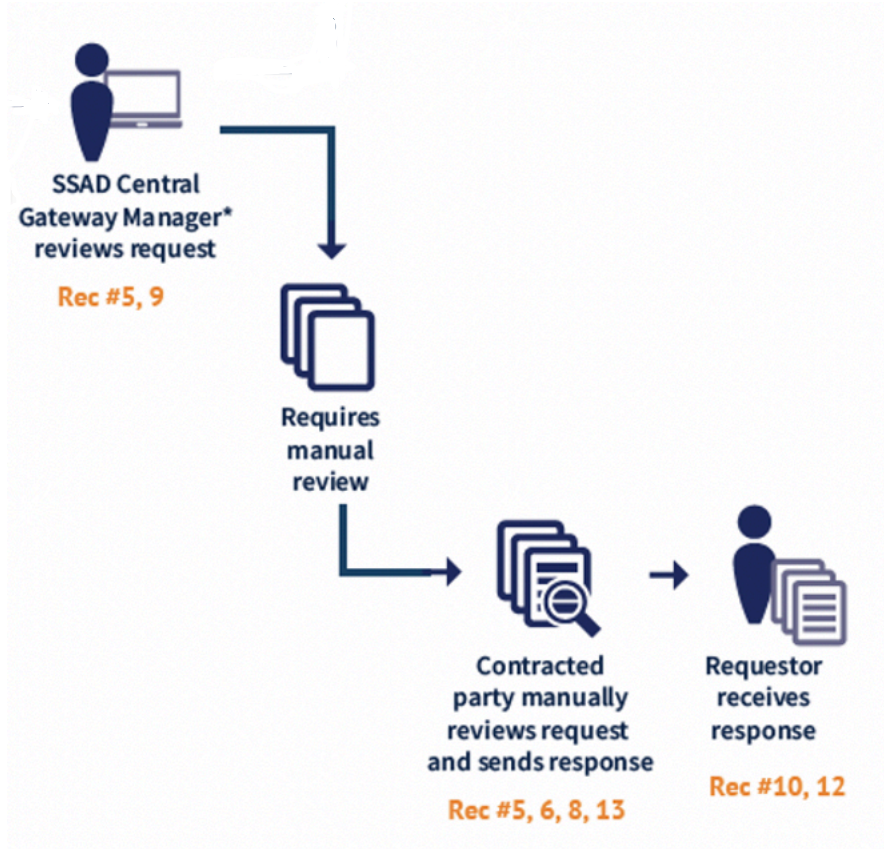
- Central Gateway receives request and must determine:
 - Is request syntactically correct?
 - Are all required fields completed?
- Following confirmation, Central Gateway Manager must send acknowledgement of receipt to requestor and relay the disclosure request to the responsible Contracted Party (the registrar of record, in most cases).
- Central Gateway Manager must also:
 - Monitor the system and take appropriate action in case of abusive use to the SSAD (such as suspending or terminating access to SSAD)
 - Support the ability of a Requestor to submit multiple domain names in a single request
 - Only support requests for current data (no data about the domain name registration's history)
 - Save the history of the different disclosure requests

Routing of SSAD Requests



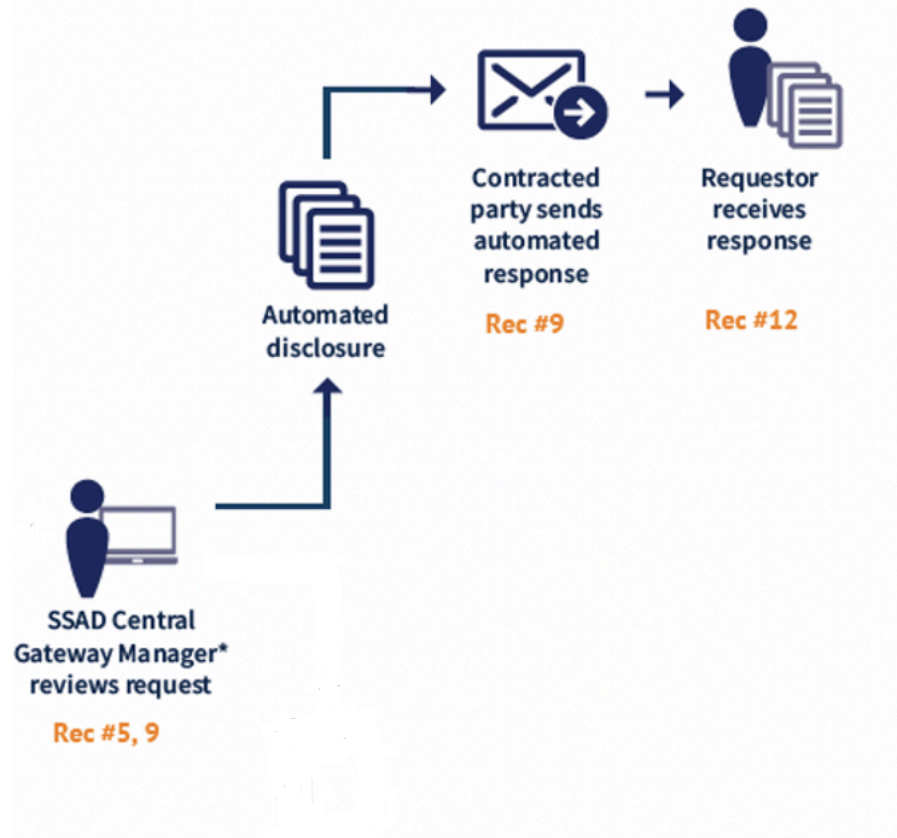
- Once a requestor submits a request to the SSAD, the request will follow one of two tracks:
 - **Automated Disclosure Track** – if the CGM confirms the request meets the criteria for automated disclosure (described in Rec. 9), the CGM will direct the CP to automatically disclose to the requestor (no review of request by CP)
 - **Manual Track** – if the request does NOT meet the criteria for automated disclosure, the CP will manually review the request and send a response to the requestor (decision to disclose rests entirely with CP – see rec #8 for further details)

Key Points of Contracted Party Authorization Requirements (Rec. 8)



- The majority of SSAD requests will follow this “manual track”
- Following receipt of a request from the CGM, Contracted Parties must:
 - Conduct a *prima facie* review – is this request valid? (Note: CGM only checks for completeness, not substance)
 - If request passes *prima facie* review, CP must review requested data elements to determine if there is personal data. If not – must disclose. If so, proceed to substantive review
 - Substantive review includes:
 - Lawful basis?
 - Are data elements necessary?
 - Further review or balancing required?
- Following substantive review, CP determines whether to disclose

Key Points of Automation (Rec. 9)



- Contracted Parties must follow the automated disclosure process in response to requests for which automation is determined to be technically and commercially feasible and legally permissible. Approved use cases based on legal memo:
 - Requests from Law Enforcement in local or otherwise applicable jurisdictions with either 1) a confirmed GDPR 6(1)e lawful basis or 2) processing is to be carried out under a GDPR, Article 2 exemption;
 - The investigation of an infringement of the data protection legislation allegedly committed by ICANN/Contracted Parties affecting the registrant;
 - Request for city field only, to evaluate whether to pursue a claim or for statistical purposes;
 - No personal data on registration record that has been previously disclosed by the Contracted Party.
- CP may opt out of automated processing by notifying Central Gateway, but only in limited circumstances (not legally permissible or significant risk).





GNSO Standing Committee Overview (Rec. 18)



- Established by GNSO Council
- Intended to review and examine data being produced as a result of SSAD operations and provide the GNSO Council with recommendations on how best to make operational (implementation) changes to the SSAD.
- Shall be composed of all groups represented in EPDP Team, including ACs.
- Recommendations concerning implementation guidance will be sent to the GNSO Council for consideration and adoption, after which they will be sent to ICANN Org.
- Recommendations concerning policy changes will be recorded by the GNSO Council for further issue scoping and policy development work or review
- Recommendations by Committee must achieve consensus to be forwarded to Council. **Support of CPs is required to achieve consensus.**

Priority 2 Recommendations (#19 - #22)

Final Recommendations – Priority 2

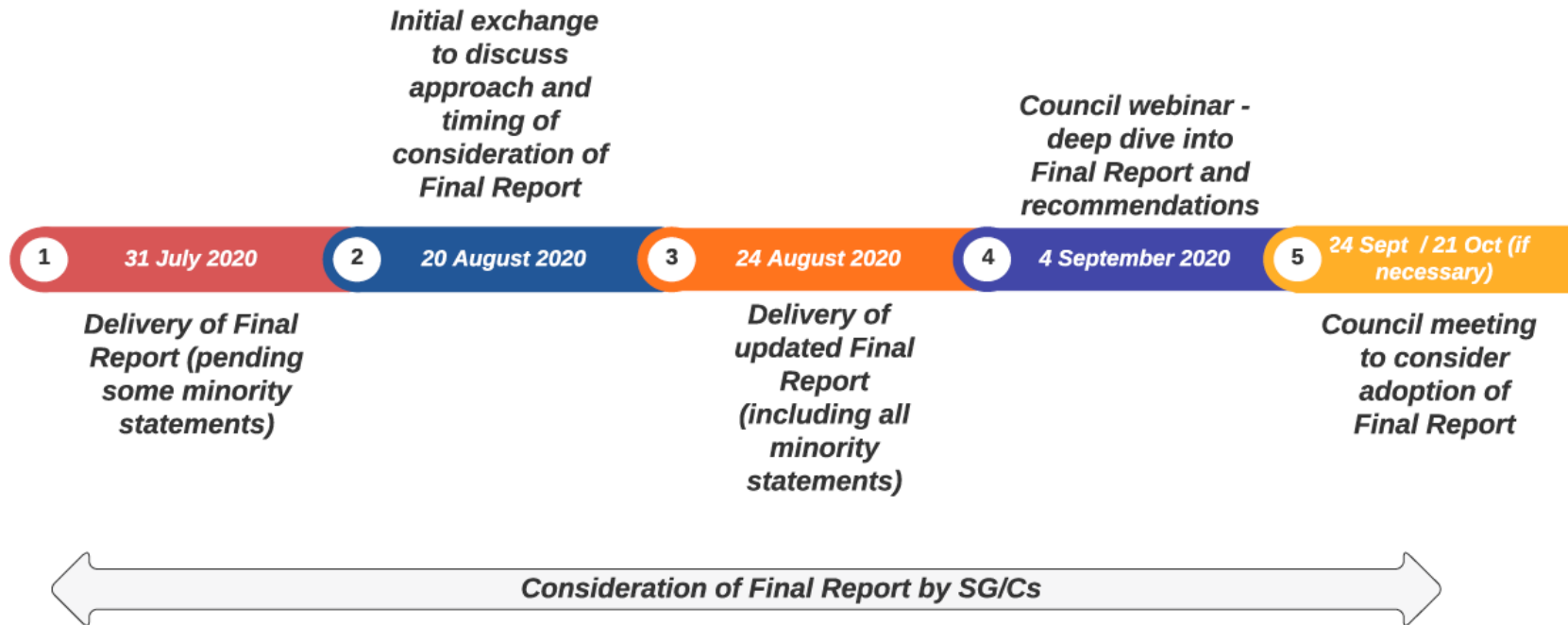
-  **#19** **Display of information of affiliated privacy / proxy providers** - provides that where it concerns a privacy / proxy registration, the data of the applicable privacy/proxy service must be included in response to an RDDS query.
-  **#20** **Redaction of City Field** – recommends updating of Phase 1 recommendation to state that redaction MAY be applied to city field, instead of MUST.
-  **#21** **Data Retention** – confirms Phase 1 recommendation that registrars MUST retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of a registration plus three months to implement the deletion.
-  **#22** **Purpose 2** – recommends addition of the following purpose to the Phase 1 purposes: “Contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN’s mission.

Expected next steps & timeline

Consensus Designations

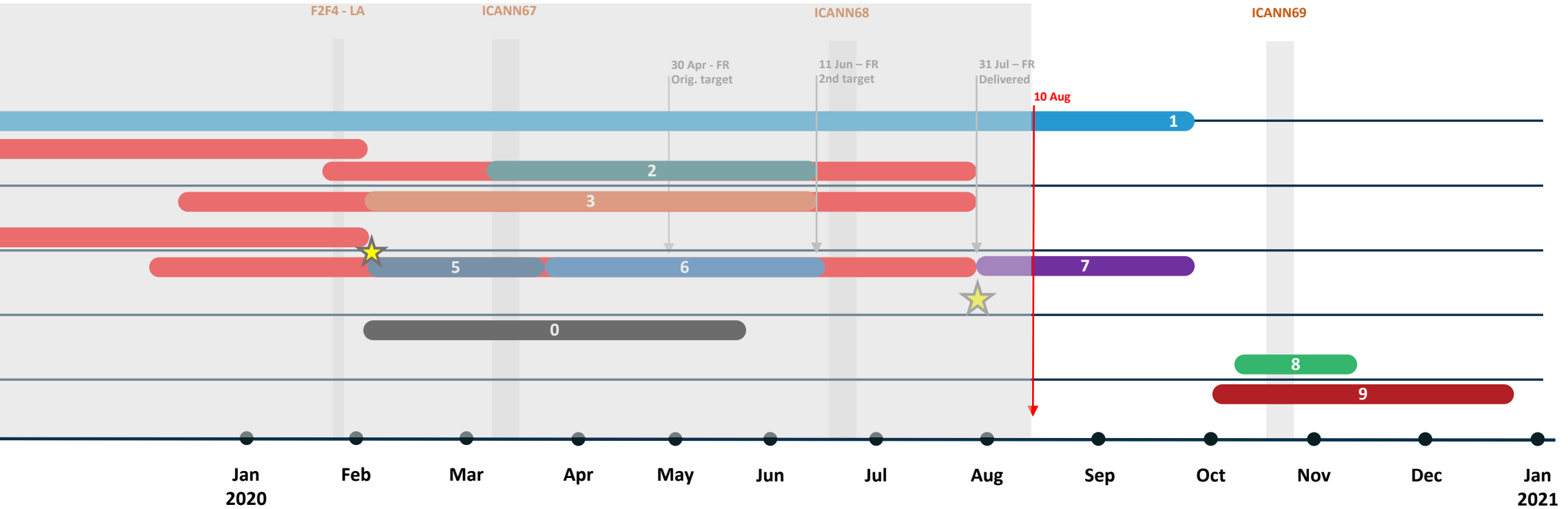
| Consensus Designation | Recommendations |
|---|--|
| Full consensus | #1 - Accreditation #2 - Accreditation of Governmental Entities #3 - Criteria and Content of Requests #4 - Acknowledgement of Receipt #11 - SSAD Terms and Conditions #13 - Query Policy #15 - Logging #16 - Audits #17 - Reporting Requirements #19 - Display of information of affiliated and/or accredited privacy/proxy providers #21 - Data retention |
| Consensus | #7 - Requestor Purposes #20 - City field #21 - Data retention |
| Strong support but significant opposition | #5 - Response Requirements (BC, GAC, IPC) #8 - Contracted Party Authorization (BC, GAC, IPC) #9 - Automation of SSAD Processing (ALAC, BC, IPC) #10 - Determining Variable SLAs for response times for SSAD (BC, IPC, RrSG, SSAC) #12 - Disclosure requirements (GAC, SSAC) #18 - Review of implementation of policy recommendations concerning SSAD using a GNSO Standing Committee (ALAC, BC, GAC, IPC) |
| Divergence | #6 - Priority levels (ALAC, BC, GAC, IPC, SSAC) #14 - Financial sustainability (ALAC, BC GAC, IPC, SSAC) |

Proposed Timeline for Council Consideration



EPDP Phase 2 - Summary Timeline

10 Aug 2020



1 Project Management, Workplan, & Factsheet

4 Construct Initial Report

7 Council Consideration of Final Report

2 EPDP-P2 Priority 1 Deliberations

5 Public Comment on Initial Report

8 Public Comment during Board Consideration⁽¹⁾

3 EPDP-P2 Priority 2 Deliberations

6 Review of Public Comment & Submission of Final Report

9 Board Consideration⁽²⁾

Complete: 97% Status: Health:

Behind Schedule

Priority 1 – Unplanned

(1)(2) best estimate on timing + duration to conclude the phase

Questions?