System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA)

25 January 2022

TABLE OF CONTENTS

List of Figures

Executive Summary

Background

Who can access data to identify individuals or entities responsible for the operation of a domain name on the Internet is an important question for many. In the Internet's early days, a registration data directory service called WHOIS provided this function. Over time, adjustments have been made to the type of registration data directory service used for this purpose, to meet the demands of today's Internet, privacy laws, and the stakeholders who use it, such as registrants, law enforcement agents, intellectual property holders, businesses, and individuals.

Following the adoption of the European Union's General Data Protection Regulation (GDPR), which required many of ICANN's Contracted Parties to redact personally identifiable information in the publicly available WHOIS, the ICANN community and the ICANN organization (org) have worked to balance the law's data protection requirements with the legitimate interests of third parties seeking access to non-public generic top-level domain (gTLD) registration data. ICANN org sought clarity from the European Data Protection Board on how the law may be applied and received feedback on several points.

The Expedited Policy Development Process (EPDP) Phase 2 team reviewed the various inputs from the European data protection authorities, as well as analysis from an outside law firm[1] to recommend the development of the system described in this document. The proposed new System for Standardized Access/Disclosure to Nonpublic Registration Data (SSAD) stems from policy recommendations made by the ICANN community that aimed to bring ICANN's Registration Data Directory Services (RDDS) into compliance with the GDPR. Eighteen recommendations for the SSAD are delineated within the Final Report of the Generic Names Supporting Organization (GNSO) EPDP Phase 2. In particular, the SSAD would facilitate the routing of requests for nonpublic gTLD registration data through a centralized system operated by ICANN org or its designee to the relevant contracted party. The contracted party, in its sole discretion, would determine whether to disclose the requested data.

ICANN org prepared this Operational Design Assessment (ODA) to aid the ICANN Board in its consideration of GNSO policy recommendations as a result of the EPDP Phase 2 work. This ODA is the outcome of ICANN's first Operational Design Phase (ODP), a tool launched in 2021 to formalize the existing process by which ICANN org assesses GNSO Consensus Policy recommendations as an input to the ICANN Board's consideration of such recommendations. The new, formalized ODP process involves estimating the resource requirements, timelines, dependencies, and risks associated with GNSO Council-approved Consensus Policy recommendations. More information about the level of effort spent by ICANN org in this ODP can be found in **Appendix 6**.

ODA Objectives

The ICANN Board directed the ICANN President and CEO to conduct the ODP and produce the ODA by addressing a series of questions about the SSAD's potential risks, anticipated costs,

[1] See: https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf, https://www.icann.org/en/system/files/correspondence/debeuckelaere-to-marby-15jan19-en.pdf, https://www.icann.org/en/system/files/correspondence/stevens-to-marby-04dec19-en.pdf, and https://community.icann.org/display/EOTSFGRD/EPDP+-P2+Legal+subteam.

resource requirements, timelines, dependencies, interaction with the Global Public Interest Framework, and other matters. ICANN org has undertaken the ODP over ten months through a transparent process, soliciting feedback from the ICANN community along the way through webinars, blogs, announcements, and via data gathering (see **Appendix 3**) and regular communication with stakeholders.

Assumptions

ICANN org set out a series of assumptions, created to provide a framework for constructing the SSAD design, roles and responsibilities of various actors, the scope of certain services and capabilities, involvement of vendors, and development of the cost model. A set of general assumptions covers the estimated number of users, the need for an accreditation process, and omission of requests for customer data held by proxy or privacy services. More detail about issues related to proxy and privacy services can be found in the General Issues section. The assumptions about the system include full outsourcing of system development and operation for the Central Gateway, and related standards for service architecture and infrastructure.

General services assumptions take into account that vendors will be selected through RFP through ICANN's standard procurement process, that blended hourly rates between $150 to $200/hour will be used for all vendor services, and that five years will be the standard contract term. Detailed assumptions (too numerous to list in this summary) related to specific functions and services such as the Central Accreditation Authority, Governmental Accreditation Authorities (AAs), Requestor Declarations, and Audit can be found in the Assessment section of this document.

Additional assumptions about timeline, resources, and staffing include the need to execute all contracts before operations begin, that ICANN org will fully fund and support the implementation work to be conducted or overseen by ICANN org, and that despite outsourcing, ICANN resources will still be needed.

Assessment

In preparing the ODA, ICANN org organized its findings and responses to the ICANN Board's questions into 12 thematic groups, described below with highlights.

Operational Readiness

This section describes how SSAD Requestors could be verified and accredited; how representatives of countries, territories, and governments could be accredited; and a discussion of legal considerations and risks. Briefly, ICANN org would outsource non-governmental identity, affiliation, and representation verification to a Central Accreditation Authority (Central AA). The Central AA would primarily use government-issued identification for identity verification and legal names, addresses, tax identification numbers, and other types of information to certify affiliation or representation. ICANN org research found several vendors claim the ability to provide identity verification in almost 200 countries.

Governmental users accessing SSAD would be verified by their country or territory's designated Accreditation Authority (AA). Each country or territory would set their desired methods for accreditation, including the designation of an AA. Countries and territories would be recognized if they are members or observers of the United Nations or are represented in ICANN's Governmental Advisory Committee. ICANN org considers the selection and appointment of one or more Governmental AAs as an internal matter for the respective governments to determine.

A number of legal considerations and risks are explored, such as legal agreements, compliance with data protection law, adaptation to evolving or future data privacy laws, litigation risk, and compliance with U.S. economic and trade sanction programs. This SSAD was designed with data protection principles in mind.

Timeline
ICANN org estimates that SSAD development and implementation will take between five and six years. This includes work, done in parallel to the extent possible, with the Implementation Review Team (IRT), which, in ICANN's previous experience, has taken up to two years and up to more than 3.5 years to develop and implement the system.

SSAD Operations
Based on the EPDP Phase 2 recommendations, the SSAD is a complex system involving 60 processes among eight types of actors, leveraged by eight different subsystems. This section describes SSAD operations at a very high level. Full detail on operational design can be found in **Appendix 1**.

For SSAD Requestors, AAs will be their only point of contact with the system. These AAs are either ICANN's designees as the Central AA, or Governmental AAs designated by respective countries or territories.

AAs relay disclosure requests through the Central Gateway, a fully automated system that routes requests to the appropriate Contracted Party for review and consideration. Review and approval may be done manually or automatically, in limited cases. Once disclosure is approved, the original Requestor may query the data from the Contracted Parties' Registration Data Access Protocol (RDAP) service.

Systems and Tools Needed
Two systems must be built to deploy SSAD. ICANN org recommends outsourcing both. One is the Central AA system, a web portal and API that will be the point of entry for SSAD Requestors to ask for data disclosure. The second is the Central Gateway System, a web portal and API for contracted parties, Accreditation Authorities, the SSAD Misuse Investigator, and web portal administrators to manage disclosure requests.

At least three existing ICANN services will need enhancements to support SSAD: the ICANN.org website, ICANN's RDAP client (lookup.icann.org), and the Naming Services portal (NSp). ICANN org assumes that a four-person insourced engineering team would handle these projects.

Vendors and Third Parties
ICANN org has identified seven vendor functions needed to operate SSAD: a Central Gateway Manager, the Central AA, an independent auditor, the SSAD Misuse Investigator, system development, customer service, and public relations services for an awareness campaign.

The steps for vendor selection follow ICANN's established procurement process. ICANN org recommends prioritizing vendor selection for the most complex and effortful work of system development. A second phase of vendor selection will fill functions such as misuse investigation, audit, and public relations.

Resources and Staffing

While ICANN org recommends outsourcing large portions of SSAD development and operations, significant time and effort will be required of ICANN org personnel, nonetheless. In this section, ICANN org describes the tasks, responsibilities, and estimates of time needed for the three phases of SSAD implementation.

Costing
Costs for development and implementation of the SSAD range from $20-27 million. Annual operating costs range from $14 million to $106 million. ICANN org presents a broad range for potential operating costs because projected volumes for accreditation identification requests and Requestor declaration verifications are uncertain and must be estimated.

Fee Structure
Three proposed fees aim to recover the costs of building, designing, and operating the SSAD. ICANN org projects a five-year payback period in its estimates.

	Low Volume	Midpoint *(average of high and low volume scenario)*	High Volume
Accreditations/Identity Verification*	$ 85.28	$ 22.22	$ 21.30
Requestor Declaration Verification	$ 190.00	$ 166.00	$ 160.00
Disclosure Request	$ 39.17	$ 0.75	$ 0.43

**Accreditations/Identity Verification includes: Natural Person Verfication, User Affiliation Verification, User Representation Verification)*

Figure ES1. SSAD fee structure based on different request volumes.

Risks
While ICANN org has not identified any SSAD conflicts with ICANN bylaws or existing policies, it does note that implementation of the SSAD recommendations would create risks, including potential liability for its operation, and litigation and regulatory inquiries arising from the SSAD. As global laws on data protection evolve, there is a risk to how the SSAD may be implemented to ensure it remains in compliance with all applicable laws.

Like any large, well-known system, the SSAD could become an attractive target to online criminals. Additional security, stability, and resiliency risks also exist around inappropriate access to personal data processed within the SSAD, so security must be a top priority.

ICANN org also identified a slate of risks specific to each area of the ODA. Of those, several key themes emerged, including complex system requirements that could impact cost, duration, and security in unexpected ways; financial sustainability due to uncertain demand; and reputational risks to ICANN stemming from actions by those critical of the system.

Global Public Interest Framework
ICANN org's analysis of the EPDP Phase 2 recommendations shows that the recommendations appear to be in the public interest. However, the ICANN Board will have additional considerations before deciding if the recommendations are within the best interests of ICANN and the ICANN community, which could call other aspects of the public interest into question. The full analysis of the EPDP Phase 2 recommendations using the Global Public Interest Framework is found in Appendix 2.

Contractual Compliance
A review of Contractual Compliance's role in SSAD operations noted that the team's primary role would be investigating complaints from Requestors or data subjects related to Contracted Parties' actions following a SSAD request. During the development and implementation phase, Contractual Compliance will need to develop processes and procedures to address complaints and interventions related to SSAD and may require additional resources based on complaint volume.

Audit
While the full scope of audits related to SSAD usage and operations will be finalized during the implementation phase, ICANN org proposes that future audits be based on compliance with established accreditation policies and procedures that will be posted via the Central Gateway. An initial audit, conducted prior to full operations, is recommended, with auditors monitoring and following up on any discrepancies or outstanding issues throughout the first and second year of operations.

Terminology and Definitions

Important terms used in this document are defined below. Some terms are drawn from the EPDP Phase 2 team's Final Report, while others are modified to accommodate the design choices proposed in this document.

Accreditation
A review process to determine if prospective SSAD users meet defined requirements. The primary mechanism for the SSAD system uses accreditation as the verification of a Natural Person's legal identification. Accreditation fees are assessed to the user. Accreditation can be maintained through the renewal process, payment of any ongoing fees, and usage of the system that conforms with the SSAD Terms of Use. Accredited users may also be referred to as Requestors.

Accreditation Authority Auditor (AA Auditor)
Third-party auditing firm contracted by ICANN org to audit the Central and Government Accreditation Authorities to ensure compliance with their accreditation policy and other requirements.

Accredited Requestor
An accredited user of the SSAD, whose identity has been verified by an Accreditation Authority (AA). Accredited Requestors are SSAD users who may request disclosure of nonpublic gTLD domain name registration data through the SSAD. Requestors identified as government entities and intergovernmental organizations may be accredited only by a Governmental AA.

Accredited Requestor Auditor
Third-party auditing firm contracted by ICANN org to audit accredited users to ensure compliance with the accreditation policy and other requirements.

Affiliation
A connection or relationship between an SSAD user and another legal entity, such as a corporation, that the SSAD user is acting on behalf of. The most common form of Affiliation is direct employment of an individual by a legal entity. Other forms of Affiliation include, but are not limited to, direct control and/or ownership of a legal entity by a Natural Person.

Audits
As outlined in Recommendation 16 of the Final Report, audits are the processes and procedures used to ensure appropriate monitoring and compliance with the requirements outlined in the Final Report.

Central Accreditation Authority (Central AA)
An entity contracted by ICANN org that has the authority to accredit nongovernmental users as Requestors in the SSAD. Governmental entities and intergovernmental organizations may only be accredited through the corresponding Governmental Accreditation Authority, and not through the Central AA.

Central Gateway (CG)
A fully automated system responsible for routing disclosure requests to the corresponding contracted parties. The Central Gateway will evaluate criteria for automated processing. It is intended that this function be fulfilled by an outsourced vendor.

Central Gateway Manager (CGM)
An entity that will operate the Central Gateway system and/or related processes. The CGM may provide support functions for Contracted Parties or AAs that need to integrate with the CG. It is intended that this function be fulfilled by an outsourced vendor.

Compliance Inquiry
A request sent by ICANN org's Contractual Compliance team to a Contracted Party to gather information, provide status on compliance violations, or monitor compliance proactively. Non-response to inquiries may result in a Compliance Notice.

Compliance Notice
A formal notification about alleged areas of noncompliance sent by Contractual Compliance to a Contracted Party. Compliance inquiries tend to precede notices if more information is required to determine non-compliance.

Contracted Party
An entity contracted with ICANN org as a gTLD registry operator or an ICANN accredited registrar and a keeper of domain name registration data.

Country/territory or Governmental Accreditation Authority (Governmental AA)
A function created by a country/territory or an entity designated by a country/territory to accredit entities that require access to nonpublic registration data for the exercise of their public policy task.

Data Subject
An individual whose identifying information is being processed as part of the SSAD. This definition covers Domain Name Contacts as well as users of the SSAD.

Designate
To select one or more parties to be responsible for one or more functions. This concept is broadly applicable and mentioned in multiple recommendations in the Final Report. Examples include the planned selection of a vendor to fulfill the responsibilities of the Central AA function. Likewise, countries and territories may select an IGO to perform AA functions for eligible governmental entities.

Domain Name Contact
A Legal or Natural Person acting as a contact for registered domain names, including the role of the registered name holder (registrant), technical, administrative, or other type of contact.

Final Report
This term refers to the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, dated 31 July 2020.

Identify
Use standard, repeatable methods to verify Legal or Natural Persons to a reasonable extent for the purposes of using the SSAD.

Identity Provider (IdP)

A vendor contracted and managed by an AA to provide identity verification or related services for one or more jurisdictions.

Implementation Review Team (IRT)
An IRT is typically formed to assist policy implementation efforts by ICANN org. An IRT is not meant to reopen recommendations, but to ensure that the implementation conforms to the intent of the recommendations.

Legal Person
Entities which are treated as persons by law.

Natural Person
A human being, as distinguished from a legal person (e.g., a corporation) created by law.

Potential Requestor
A user that has not yet been accredited by an AA.

Public
Public Internet users.

Qualifying Electronic Identification (eID) System
Qualifying Electronic Identification Systems have the following characteristics:

- Used at a significant scale in one or more jurisdictions.
- Used for transactions of significance in legal, financial, and healthcare sectors.
- Subject to regulation or substantial public scrutiny.
- Available for private entity use.
- Meet or exceed the expected verification methods proposed for the SSAD.

Representation
The state of an SSAD user who is not in an affiliated relationship but is using the system on behalf of a legal entity. Examples of Representation include attorneys acting on behalf of a client, an individual performing brand management or protection services, etc. It is possible for an SSAD user to have affiliation and representation relationships concurrently. An example of this would be a user who is directly employed by an organization that provides services that benefit from the use of the SSAD to other organizations in a vendor relationship.

Requestor
An accredited user in the SSAD who has had their identity verified and has a currently active account. May also be referred to as an Accredited Requestor.

Requestor Declarations
Characteristics of Natural or Legal Persons that may be applicable to requests for nonpublic registration data. An example is trademark ownership/control. The term “Signed Assertions” was specified in the Final Report. However, assertions are also a term used in various technical frameworks that were considered in the proposed design. To avoid confusion between the different uses of the similar term, the term “Requestor Declarations” has been used throughout the document.

RDAP Service Operator

The entity that operates a Registration Data Access Protocol (RDAP) service for disclosing domain name registration data. This entity may be the Contracted Party itself or a third party acting as the Contracted Party's service provider.

Software Development Lifecycle (SDLC)
Describes one of many processes that is used in the software industry to design, develop, test, and deploy software.

SSAD (System for Standardized Access/Disclosure)
The SSAD is the overall suite of parties and parts that make up the request, review, and disclosure system. It is an overall amalgamation of systems, not one specific system.

SSAD Misuse Investigator
A function to monitor and verify potentially abusive behavior or practices by Requestors in the SSAD, as well as recommend corrective measures against abusive behavior. It is intended that this function be fulfilled by an outsourced vendor.

Terms of Use (ToU)
An agreement between users of a system or service that includes the scope of the services provided, any limitations on usage, and any related requirements or restrictions. Before being able to use the SSAD, all users will need to agree with the Terms of Use.

1 Assumptions

ICANN org created the following set of assumptions to provide a framework for constructing the SSAD design, roles and responsibilities of various actors, the scope of certain services and capabilities, involvement of vendors, and development of the cost model.

1.1 General Assumptions

ICANN org assumes the following estimated user and system capacity levels[2] as a basis for developing potential system design/capacity and costs for infrastructure and customer support operations:

- Between 25,000 and 3 million users.
- Between 100,000 and 12 million requests submitted annually.

The SSAD will only support accredited Requestors. In other words, a potential Requestor must be accredited before they can submit a request in the system.

The SSAD would not be built to process requests for customer data held by proxy or privacy services. In the event future policy discussions result in consensus that SSAD should be used to solve proxy or privacy review and disclosure challenges, additional resources would be needed to enhance the SSAD accordingly.

The SSAD, and the persons and entities operating and using it, must comply with all applicable laws. Each person or entity bears its own responsibility for this.

For this ODA, ICANN org did not:

- Estimate costs for Contracted Parties' systems development and operation, or any other indirect costs.
- Estimate costs for Requestors' systems development and operation, or any other direct or indirect costs.
- Estimate costs to governments to create an accreditation program, designate an AA, or integrate with the SSAD.
- Include risk mitigation costs, including estimates for a legal risk fund, which are variable depending on what role ICANN org is slated to play in the final model.[3]
- Estimate costs associated with potential ICANN accountability mechanisms.

1.2 System Assumptions

The ODA assumes full outsourcing of system development and operation for the Central Gateway and systems that support the Central AA.

[2] ICANN org examined several inputs to arrive at an estimated range. The data used included contracted party surveys (see Appendix 4), community surveys (see Appendix 5), a consideration of the rate of potential SSAD misuse, previous inputs from the EPDP Phase 2 Working Group and estimated numbers of law enforcement around the world. More information about data collection can be found in Appendix 3.

[3] Recommendation 14.4 of the Final Report notes: “Funding for the SSAD should be sufficient to cover costs, including for subcontractors at fair market value and to establish a legal risk fund.” Should the Board direct ICANN org to implement the SSAD, further discussion will be required regarding a possible legal risk fund.

For estimation purposes, ICANN org used person-hours to measure functional complexity. A price of $200 per person-hour was calculated for both insourced and outsourced professional work, along with an estimated team structure and size.

ICANN IT guidelines for third-party vendors will be followed. All hosting infrastructure will be external and follow ICANN's E&IT service architecture and infrastructure requirements while supporting ICANN accessibility and universal acceptance standards. The user interface for the systems created by ICANN org and its designees will be in English.[4]

1.3 Services Assumptions

For all services assumptions noted, three general premises were applied. First, vendors will be selected via RFP through ICANN org's standard procurement process as applicable under ICANN's procurement policy. Second, the blended hourly rates for all services including audit, the Central AA, SSAD Misuse Investigator, etc., are assumed to be between $150 and $200/hour, depending on the function. Third, that five years is used as a standard contract term, where applicable.

Below, assumptions are arranged by different elements of the SSAD.

Central Accreditation Authority (AA)
The SSAD will support accreditation requests from anywhere in the world, to the extent permitted by applicable law, available identity documentation, available standards for review identity documentation, and Internet access.

Natural Persons who wish to become accredited must have reached the age of majority in their local jurisdiction before they can apply.

Renewal of Accreditation of Natural Persons will occur at least every two years. Verification of Legal Persons, Representation, and Affiliation will occur at least every five years.

There will be some information and documentation related to the legal entity required to demonstrate Affiliation and/or Representation with legal entities.

Legal Persons will be verified by electronic means whenever possible.

The Central AA will not accredit governmental entities or intergovernmental organizations (IGOs).

The identity verification methodology model is strictly limited to identifying a Legal or Natural Person. It does not incorporate qualitative review of applicants, such as conducting background screening.

If the Central AA requires a vendor to provide identity verification services, it may contract with one or more identity providers (IdP) that provide related services.

Governmental Accreditation Authorities (AA)

[4] Per Implementation Guidance 3.5 in the Final Report, "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)."

Countries and territories may choose to participate in the SSAD. Full participation is required to obtain all functionality of the SSAD, including automated disclosure of data. To be full participants, countries and territories must meet all applicable recommendations within the Final Report, specifically Recommendation 2, which also incorporates Recommendation 1.3. This means that countries and territories who want to participate in the SSAD are assumed to have committed to:

- Creation or designation of an AA for the country/territory.
- Funding of any operational or technical costs.
- Development of systems and interfaces to integrate with SSAD systems.
- Technical integration with SSAD systems and interfaces to facilitate secure exchange of information and credentials.
- Verification of requestor declarations for applicable law enforcement users.
- Provision of an interface for its own accredited users to request data, including appropriate validations.

ICANN will publish the technical interfaces and requirements for country/territory AA integration. A single version of technical interfaces will be provided to all AAs and IdPs (as applicable).

Requestor Declarations (known as Signed Assertions in the Final Report[5])
Verification of trademark ownership will leverage the existing Trademark Clearinghouse (TMCH) standards and mechanisms. Trademark verification will be subject to established TMCH fees for trademarks that are not currently active in the TMCH. Trademarks must remain active in the TMCH for the Requestor Declaration to be valid.

Audit
ICANN org assumes that the following parties will be subject to audit[6] of their SSAD usage and operations, as outsourced to one or more vendors:

- Accreditation Authorities.
- Identity providers.
- Accredited Requestors.

ICANN org will contract with a third-party auditing firm to act as the AA auditor of the central and Governmental AAs. AAs will be tasked with auditing any identity provider; therefore, such responsibilities and results will be included in the Audit of the Accreditation Authority.

ICANN org will also contract with a third-party auditing firm to act as the accredited Requestor auditor. The contracted firm will jointly work with ICANN org to develop an audit program that will be implemented. The firm will conduct audits per the requirements of the audit program and produce appropriate documentation.

In the case of AAs, an initial audit must be conducted prior to becoming fully operational. During the rest of the first and second year, the auditors would monitor and follow up on any discrepancies or outstanding issues. Subsequent audits will focus on collecting evidence based

[5] The term “Signed Assertions” was specified in the Final Report. However, assertions are also a term used in various technical frameworks that were considered in the proposed design. To avoid confusion between the different uses of the similar term, the term “Requestor Declarations” has been used throughout the document.
[6] As outlined in Recommendation 16 of the Final Report, audits are the processes and procedures used to ensure appropriate monitoring and compliance with the requirements outlined in these recommendations.

on a risk and materiality analysis, including reports of any internal audit conducted by the AA and general assessments of Audits to ensure the internal audit works as intended.

Governmental Accreditation Authorities will have the option to either be audited by the contracted Accreditation Authority auditor, or to have an audit done independently, with the report provided to ICANN org.

The proposed audit process is primarily a review of the various system logs generated as a result of user activity. It is not contemplated that the auditor would conduct on-site visits or reviews of private systems to verify compliance with all terms of use.

The more languages supported in the ecosystem of SSAD, the more costly the audit process will be.

1.4 Timeline Assumptions

Data protection and other legal agreements (where required) and related documents among the parties (vendors, Contracted Parties, designated Country/territory AAs, etc.) must be fully executed before the SSAD can begin operations. ICANN org will work to complete implementation activities in parallel to the extent possible.

1.5 Resources and Staffing Assumptions

While ICANN org proposes fully outsourcing this work, internal resources will be assigned to provide service/product ownership and oversight of system development, ongoing operations, and audits of CGM and AAs.

ICANN org will fully fund and support the implementation work for the project's duration.

2 General Issues

In this section, ICANN org explores an array of general issues to be considered. For example, the existence of privacy and proxy services that protect domain registrant identity from public access complicates the SSAD Requestor experience in several ways, which are listed below. Further in this section, readers will find descriptions of other issues that may arise, such as changing laws and regulations, and the need to de-accredit a Governmental AA.

2.1 Privacy and Proxy Services

The proposed SSAD implementation approach assumes the system will only handle base-case requests for data for non-proxy/privacy service registrations.[7] However, the existence of proxy and privacy services poses several challenges to the system's operations, which are explored in the following paragraphs.

It is important to note that the guidance of the EPDP Team is to provide a mechanism to label privacy/proxy registrations so that it is clear for Requestors where to direct their disclosure requests.[8] SSAD Requestors may feel confused or frustrated with the system if they don't receive the registrant data they seek due to proxy or privacy service use. Planning for this and mitigating the effects will be key during process design and drafting of request forms and user instructions.

During its design work, ICANN org applied a working assumption that at least 30% of registered domain names make use of a proxy or privacy service and will not yield results through an SSAD request for non-public data. This may be a conservative estimate, based on a January 2021 study. However, data is limited, and it is difficult to know the full impact of proxy and privacy services on potential SSAD use. For example, if a significant percentage of requests are for registrant information shielded by a privacy or proxy service, this may call into question the estimates of volume, accreditation, usage, and renewal.

Adverse Impacts

Additionally, SSAD Requestors may have a negative experience using the system if the data they seek is protected by a privacy or proxy service. For example:

[7] Requests submitted via the SSAD can only concern the gTLD registration data elements identified by the EPDP Team (e.g., registrant name, registrant postal address, registrant email address, etc). In the case of a domain registered using a proxy registration service, all the gTLD registration data (e.g., data of the proxy service) is already required to be public. The contact data pertaining to the beneficial user of the domain (the proxy service) could not be requested via the SSAD. With respect to domains utilizing a privacy service, all gTLD registration data (e.g., the contact data provided by the privacy service) is, again, already required to be public. However, the registrant's name would be potentially redacted, because in the case of a privacy service, the registrant of record (i.e., the privacy service) remains the beneficial user of the domain name. Thus, requests for registration data pertaining to a domain protected by a privacy service could be submitted via the SSAD and would be considered by the applicable registry/registrar as all other requests for nonpublic gTLD registration data but could only potentially concern the Registrant Name field.

[8] EPDP Phase 1, Recommendation 19 requires registrars who operate an affiliated privacy or proxy service to publish the full nonpersonal RDDS data of the privacy/proxy service, to help avoid a scenario where users request data for a registration that utilizes a privacy or proxy service. This could reduce the likelihood of a requestor submitting a request for data concerning a privacy/proxy-protected domain.

- An SSAD Requestor may pay fee(s) to request registration data, only to be provided a limited response, such as the registrant's name only (in the case of a privacy service), the privacy/proxy name and contact information, or no data at all. Requestors would need to submit another data disclosure request to the privacy and proxy service provider, outside of the SSAD.
- An SSAD Requestor may experience longer-than-usual waiting times. In the most common case, SSAD requests submitted to the SSAD will be subject to various Service Level Agreements (SLAs). However, these SLAs for disclosure of nonpublic registration data do not apply to a privacy or proxy service's evaluation of a request.

These outcomes could result in significant user confusion and/or dissatisfaction, and could lead to one or more of the following:

- High volume of complaints and/or demands for refunds.
- High volume of customer service inquiries/requests.
- High percentages of non-renewal for SSAD Requestors, resulting in fewer users of the system.
- Users discouraging others privately or publicly from obtaining accreditation.

The immediate implementation of the GNSO's 2015 policy recommendations on Privacy and Proxy Service Accreditation Issues (PPSAI) would not remedy this situation because:

- The policy recommendations concerning request evaluation processes and timelines in PPSAI and the Final Report are not aligned.
- There are no required disclosure evaluation or balancing processes in the PPSAI policy recommendations.
- The PPSAI recommendations, as they were developed prior to the EPDP's establishment, do not address the issue of SLAs in a scenario where a request was routed under the SSAD process, but concerns privacy/proxy customer data.

Relevant Policy Recommendations

The EPDP Phase 2 Team did not address how the SSAD should interact with requests for customer data held by proxy or privacy services, if at all, as this question was not in the scope of the team's work.[9]

[9] Specifically, the EPDP Team was asked to consider the text of the Temporary Specification, and the Temporary Specification did not address access to the underlying data of customers utilizing privacy or proxy services.

The sole reference to privacy/proxy services within the Temporary Specification appears in Section 2.6 and provides, in part, "in the case of a domain name registration where a privacy/proxy service used (e.g., where data associated with a natural person is masked), Registrar MUST return in response to any query full WHOIS data, including the existing proxy/proxy pseudonymized email." The EPDP Team did review this text, as part of its charter, and put forward Recommendation 14 (Phase 1 Final Report) and Recommendation 19 (Phase 2 Final Report). These recommendations from the EPDP Team endeavor to make clear that privacy or proxy data must not be both redacted and shielded via a privacy or proxy service. In other words, the full privacy or proxy data (e.g., privacy@privacy.example) must be displayed in the RDDS so that Requestors are notified, via RDDS, to request underlying customer data via the privacy/proxy service rather than through the Registrar or Registry.

Following the EPDP Team's work on Recommendation 19 during Phase 2, the EPDP Team, via its ICANN org support staff team, notified the ICANN org liaisons on 11 March 2020 that, "the EPDP Team has concluded its deliberation on P/P services. While this recommendation will go out for public comment and eventually go to the GNSO Council and Board, the EPDP Team believes that its work with respect to

The Privacy and Proxy Service Accreditation Issues Working Group (PPSAI WG) did not have the opportunity to address this topic, given that its recommendations were developed prior to the EPDP. The PPSAI WG recommended that ICANN org implement an accreditation program for privacy and proxy service providers. The accreditation program requirements recommended by the PPSAI included criteria for providers' receiving and responding to requests for privacy/proxy customer data. It is possible that the PPSAI recommendations concerning this process, at least with respect to registrar-affiliated privacy and proxy services, could be streamlined via full or partial integration with the SSAD, when modified accordingly to account for such purposes.

2.2 Other Issues

Several other issues arose during the ODP as having potential impact on implementation of the GNSO Council-approved policy recommendations related to the SSAD and these are noted here.

Timely Responses

First, there is no standard duration or SLA from when the Contracted Parties approve a request to when they must allow Requestors access to the requested data. There are also no required standards within the Final Report as to the required length of time for such access. In addition, the Final Report does not provide details on how the Contracted Parties must support reexamination requests in terms of a specific SLA.

Changing Laws and Regulations

The legal environment in which the SSAD and its users (Requestors and Contracted Parties) will function is fluid. New laws and regulations could impact SSAD usage and its operation in the future.

As noted in many recent submissions to European lawmakers and regulators, ICANN org believes there are uncertainties regarding how the GDPR applies to the processing of registration data. ICANN org can and will implement the SSAD based on an informed understanding of the requirements of the GDPR and other applicable laws if directed to do so by the Board; nonetheless, SSAD implementation (and the broader ICANN ecosystem) would benefit from added regulatory clarity. Continued outreach to the relevant data protection authorities with respect to the SSAD could provide additional feedback and clarity to inform the design and approach to implementing data protection arrangements that may be required under applicable law.

De-accreditation of Governmental AA

P/P is complete for now. Although input as a result of public comment may result in changes to this specific recommendation, the EPDP Team will not consider any other aspects of P/P beyond what is captured in this recommendation."

Following ICANN org's delivery of the Wave 1.5 Report on EPDP Phase 1 recommendations, which identified areas of the PPSAI recommendations potentially impacted by the EPDP Phase 1 recommendations, ICANN org asked the GNSO Council to identify which, if any of these areas, would require updates to the PPSAI recommendations. The GNSO Council responded noting that "based on the analysis and the impacts identified in the Wave 1.5 report, there appears to be no required updates or any bar to continuing the implementation of the original policy recommendations."

Recommendation 2 includes the possibility that a designated Governmental AA could be de-accredited. However, the recommendation does not include mechanisms to revoke eligibility for a de-accredited Governmental AA. Thus, a country/territory could designate a previously de-accredited AA. ICANN org does not have any authority or basis upon which to evaluate, approve, or decline the designation of an AA by a country/territory.

3 Assessment

This section provides an overview of ICANN org's assessment of how the GNSO Council-approved policy recommendations related to the SSAD could be implemented. The segments below are organized by 12 work areas and meant to provide an understanding of ICANN org's approach.

3.1 Operational Readiness

Planning for how the SSAD could perform on day-one of operations began with a look at potential system users. Specifically, ICANN org examined how users of the system could be accredited to request access to personal data about domain name registrants. Issues related to user accreditation are explored below.

3.1.1 Accreditation, Including Identity Verification

Below is the proposed process to determine if prospective SSAD users meet defined requirements for system use.

3.1.1.1 Scope

ICANN org will designate a Central AA that will be responsible for identity verification of Natural and Legal Persons using the SSAD in a non-governmental capacity. Governmental users in the capacity of a public policy role will need to be verified by country/territory-designated Accreditation Authorities that will be fully separate and distinct from the Central AA.

Accreditation Authorities have the responsibility to verify identity in different jurisdictions. The Central AA has the broad mandate to offer such services as widely as possible and thus may need to select and work with additional parties to provide identification services. These parties are known as identity providers (IdP) in the Final Report. Accordingly, the criteria for selecting such providers will be determined by the selected Central AA vendor. Each vendor will have differing internal capabilities, partners, and plans that would require a unique approach to selecting their own vendors and could include criteria such as cost, availability, jurisdictional coverage, technology, service capabilities, prior experience, etc.

It is important to note that whatever mechanism is implemented, no method can be completely foolproof. Rather, the recommendations in this area represent a balance of three key elements: the cost of identity verification (driven by the level of required review by vendors), effort required by applicants (itself a balance of materials required and amount of effort needed), and the sensitivity of the data being requested via the SSAD.

3.1.1.2 Design and Operations

This section focuses on the processes and documents that could be used to accredit users.

3.1.1.2.1 Natural Person Verification

The Central AA will incorporate qualifying Electronic Identification (eID) systems where possible. Qualifying eID systems will be those that are used at scale in one or more jurisdictions for transactions of significance, including legal, financial, and healthcare. Further, such systems will need to be subject to regulation or public scrutiny and must be available for private entity use. The AA will evaluate available eID systems to ensure that they meet these criteria and have

sufficient identification methodology such that they meet or exceed the proposed verification methods below.

When an applicant does not have access to a qualifying eID, the Central AA will perform identity validation using a government-issued photo ID. The provided documentation will be analyzed to ensure it matches the characteristics of the official document. Furthermore, an electronic process will occur to ensure that the applicant is a live human being (a concept called "liveness") who matches the photo on the identification document. If the identification document has electronic capabilities (e.g., an embedded chip), the ideal situation will be to leverage any verification capabilities if available to private industry. See **Figure 1.**

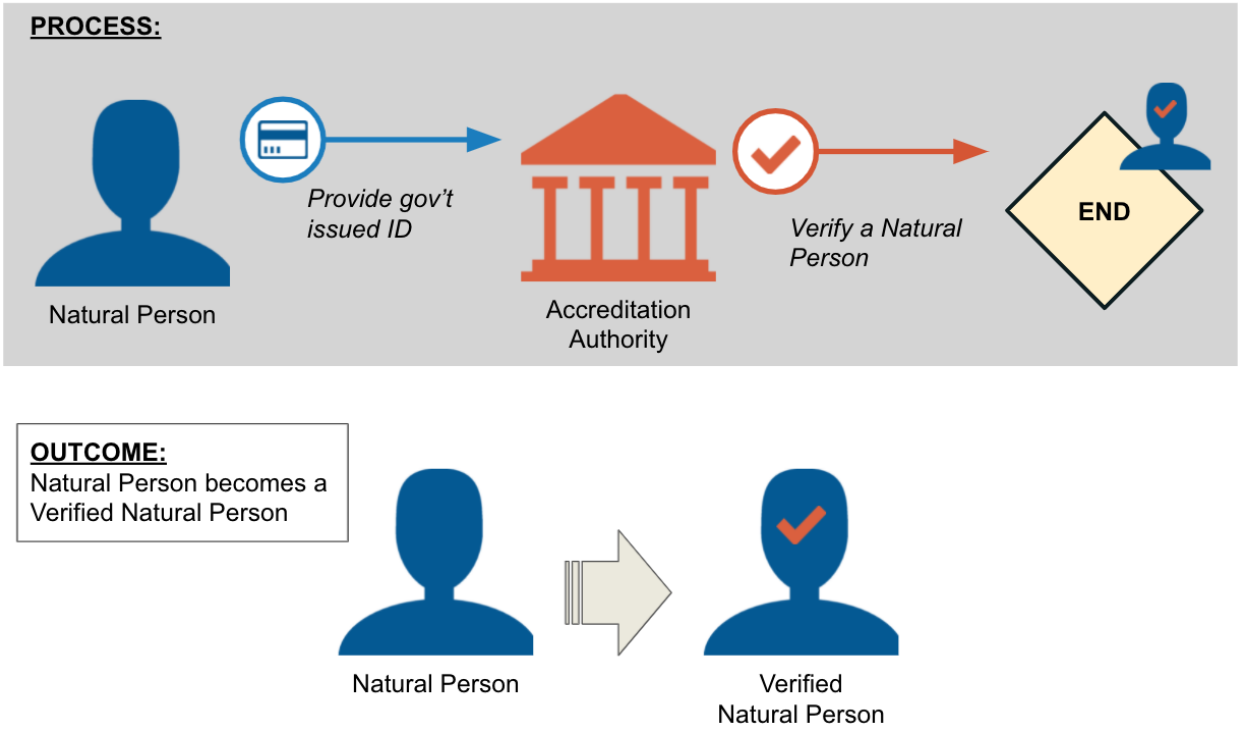

Figure 1. Verification of a Natural Person.

The Central AA may contract with identity providers as needed to offer such services as broadly as possible. ICANN org research (see Appendix 3) found several vendors that claimed the ability to provide identity verification in almost 200 countries.

Just as not every Natural Person in the world has Internet access, not everyone in the world has a valid, government-issued identification document. However, given that identification is largely a function of governments, a requirement for such documentation is a needed foundation.

The Central AA will offer an appeals mechanism for unverifiable applicants.

Natural Person verification will be valid for up to two years. If the underlying documentation is not valid for the entire two-year period, the initial accreditation period may be shorter. Verified users do not automatically receive any data. Instead, verification allows them to request nonpublic registration data.

3.1.1.2.2 User Affiliation Verification

Individual SSAD users must declare their Affiliations with any Legal Persons. SSAD Terms of Use (ToU) will spell this out and require user acceptance before granting system access. While affiliation is not specifically defined within the Final Report, generally, affiliation is assumed to be related to employment with the legal entity or control or ownership.

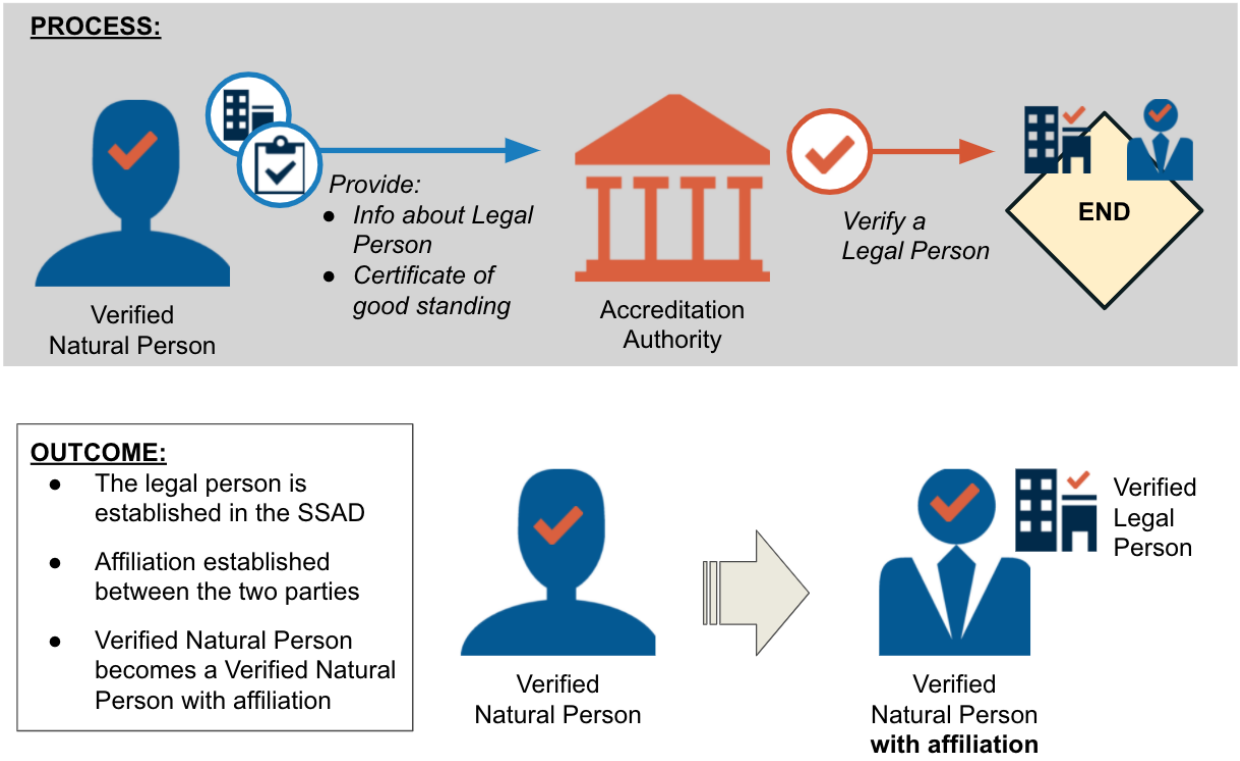

Figure 2. Verification of a Legal Person.

Affiliation verification may begin once a user has been individually verified and has accepted the ToUs. At this point, the user will be able to start a process that allows them to provide information about the legal entity and their relationship. Examples of the required information include, but are not limited to, the legal name of the entity and any "doing business as" names, the full address, and tax or other identification number. Also required would be a recent document demonstrating good standing (up to date on fees, not suspended or in a similar state, etc.) with the appropriate authority.

When received, the Central AA would conduct electronic verification(s) possible on the combination of information provided and jurisdiction. After the Central AA validates the documents as authentic, the Legal Person is added to the system. The verified person who provided the information could then verify Affiliation with that legal entity for other users of the SSAD. See **Figure 2**.

Legal Persons within the system would be renewed (re-verified) every five years. Users who misuse the system will be subject to graduated penalties and such penalties may extend to users who share the same Affiliation.

3.1.1.2.3 User Representation Verification

Requestors who use the system to request data on behalf of another party (e.g., an attorney representing a client) must declare who they represent. This requirement will be part of the

SSAD system ToUs that users must view and accept prior to system use. While representation is not specifically defined within the Final Report, generally, representation is assumed to be an indirect, non-employment scenario, such as outside legal counsel or a service firm such as brand protection.

The process for verifying representation will be similar to the process followed for verifying affiliation. However, in the most typical case, there will be no user within the system who has gone through the identity verification process and can verify an SSAD user as representing the legal entity. After all, the typical motivation for representation is to have someone else perform specific functions. As a result, representation verification will require an additional verification step of an individual who can provide information on the represented Legal Person and verify that the user in question does represent them.

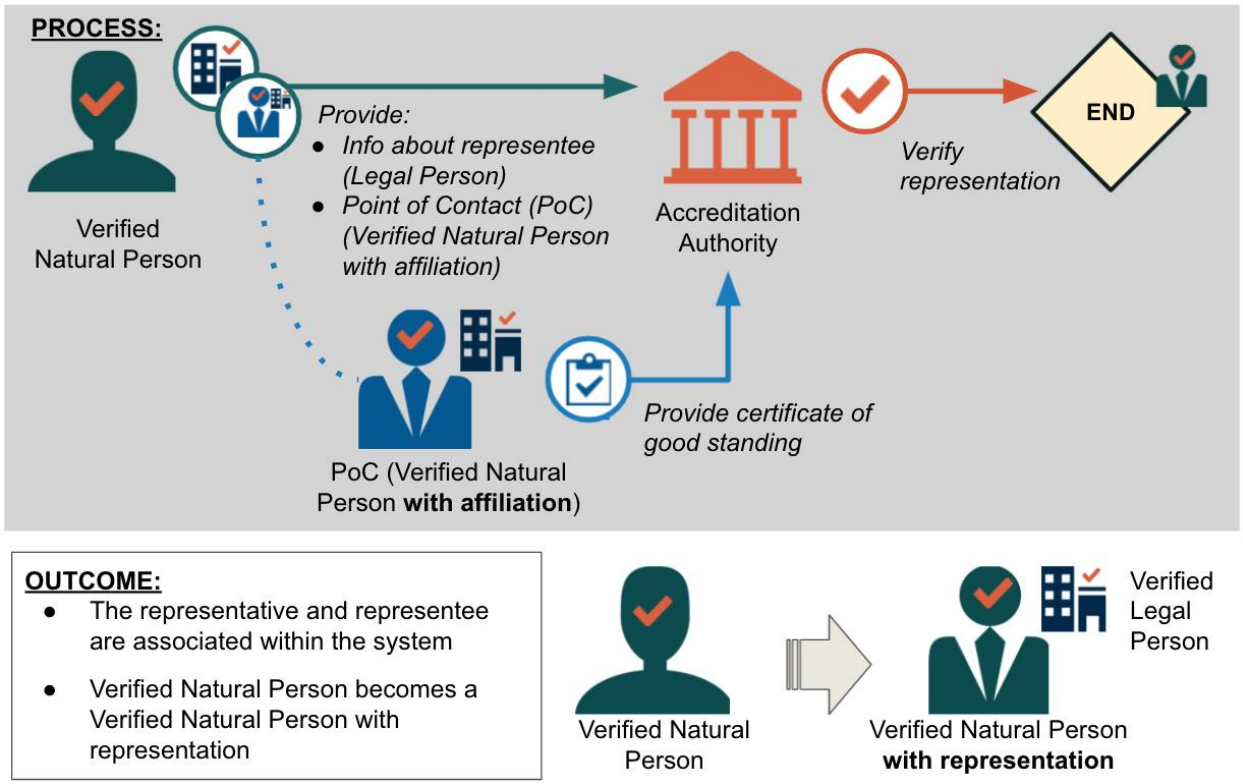

Figure 3. Verification of a Natural Person with Representation.

Representation verification may begin once a user has been individually verified and has accepted the ToU. At this point, the user provides information about a point of contact at the organization they represent. That individual point of contact must verify their identity via the Natural Person identification verification process previously described. Once verified, they will need to provide detailed information about the Legal Person. Examples of the required information include, but are not limited to, the legal name of the entity and any "doing business as" names, the full address, tax, or other identification number. The process also would require a recent document demonstrating good standing (up to date on fees, not suspended or in a similar state, etc.). See **Figure 3**.

When received, the Central AA would conduct reasonable and available electronic verification(s) of information provided and jurisdiction. Once the Central AA has validated the

documents as authentic, the Legal Person is added to the system. The verified person who provided the information on the Legal Person could then potentially verify representation of that legal entity for other SSAD users.

Legal Persons within the system would be renewed (re-verified) every five years. Users who are determined to have misused the system will be subject to graduated penalties and such penalties may extend to users who share the same representation.

3.1.1.3 Implementation Considerations

ICANN org plans to outsource the Central AA function. However, outsourcing still requires effort to define the nature of the vendor's responsibility, create a contract specifying the same, and conduct a request for proposal (RFP) to find a vendor to carry out those obligations. These key milestones are listed below and more information on implementation is available in the Vendors and Third Parties section.

- In consultation with the IRT, develop explicit requirements for the Central AA function including roles and responsibilities, functional obligations, required methodologies, service level requirements, and requirements for any subcontractors.
- Develop RFP content to include the requirements listed above, a scoring system to objectively evaluate responses (where possible and appropriate), and any communications required to attract bidders.
- Conduct the RFP, respond to questions, and evaluate all responses to select the most appropriate bidder.
- Negotiate and contract with the winning bidder.

Lastly, at launch, it is not expected that user groups or categories of user groups will be part of the accreditation process. It is possible that during the IRT phase, or after gaining experience with accreditation, that user groups/categories could be defined such that they may offer value to the accreditation and potentially the disclosure review.

3.1.1.4 Risks

The following risks relate to the Central AA.

Risk Name	Consequences	Proposed Controls/Mitigation
Incorrect identification	The Central AA or a contracted IdP incorrectly verifies the identity of a Natural Person or incorrectly validates the existence of a Legal Person.	Contracted Parties can notify ICANN org of an abusive or potentially abusive user. Regular audits will occur of AAs and system usage to find patterns that may represent misuse of the SSAD.
Unable to identify users	The Central AA or a contracted IdP unable to identify a natural person.	An appeals mechanism will be available to applicants.
A user does not declare Representation or Affiliation	The activity of a user who becomes abusive will not correctly accrue to affiliated and represented Legal	Terms of Use will require such disclosure. Anyone who becomes aware of an abusive user may report the issue for investigation.

Risk Name	Consequences	Proposed Controls/Mitigation
	Persons and thus penalties will not be properly applied.	The abusive user will be subject to penalties up to and including revocation of user access.

3.1.1.5 Issues Requiring Further Development

Footnote 11 of the Final Report specifies that a user who represents other entities must disclose such applicable relationships. While ICANN org expects to incorporate this requirement into the SSAD ToU, additional methods to reduce the potential for misuse have not been determined.

3.1.2 Country/Territory/Government Accreditation

Specific considerations apply when it comes to accreditation of governmental entities. This section takes these particular issues into account.

3.1.2.1 Scope

Accreditation for governmental entities is subject to the requirements in Recommendation 2, which also incorporate some requirements from Recommendation 1.

Countries and territories will largely be able to define their desired methods for accreditation including the creation or selection of an Accreditation Authority (Governmental AA). Eligibility is defined in Recommendation 2 and includes individuals and entities that "...require access to nonpublic registration data for the exercise of their public policy task…" Accordingly, this ODA does not provide any specific design elements for a Governmental AA beyond those offering technical and systems support.

3.1.2.2 Participation by Countries and Territories

The Accreditation of countries, territories, and governments leads to the question of what constitutes a country or a territory. In other words, how are countries or territories recognized so they will be able to designate an AA? ICANN org proposes that countries and territories that are members or observers of the United Nations (U.N.) and/or are represented in ICANN's Governmental Advisory Committee (GAC) may designate a Governmental AA.

The recognition of a state or government is an act that only other states and governments may grant or withhold. The U.N., as an organization of independent states, includes states or governments in its membership (and may admit a new state to its membership or accept the credentials of the representatives of a new government). It furthermore includes observers from non-member states and intergovernmental and other organizations.[10]

3.1.2.3 Designation of a Governmental Accreditation Authority to ICANN org or Its Designee

The selection and appointment of a Governmental AA or creation of a new body to take up this role is an internal matter for the respective governments.

[10] According to Recommendation 2, the role of a Country/Territory AA can be delegated to an IGO.

The designation of a Governmental AA to ICANN org or its designee should be communicated by each country or territory's Ministry of Foreign Affairs or agency with a similar competency and scope, unless the country or territory is represented in the Governmental Advisory Committee (GAC), in which case the designation should be communicated by the GAC representative.

While the GAC includes 179 members and 38 IGO observers, it does not include all countries of the world. At the same time, different countries allocate different competencies within a government and have different governmental structures. ICANN org is in no position to know which is the competent body or authority in each country from which to accept a designation for countries/territories that do not participate in the GAC. The function that is common for all countries or territories is diplomatic relations (external representation). ICANN org therefore proposes that, for those countries/territories that are not part of the GAC, the designation of a Governmental AA is communicated by their Ministry of Foreign Affairs (or equivalent).

More than one AA can be designated by a country/territory. Each country/territory should be able to designate as many AAs as necessary according to its national conditions.

3.1.2.4 Implementation Considerations

Individual countries and territories will determine the implementation of Governmental AAs. However, per the Business Process Design, the accreditation function will depend on certain capabilities that would be built as part of the SSAD systems.

ICANN will publish and support the technical interfaces that the Governmental AA will use to integrate into the SSAD. The intent would be to publish interface specifications once the design is finalized so as to allow time for countries, territories, and/or their designees to begin design and implementation of supporting systems.

In a webinar with the GAC that was focused on governmental accreditation as part of the proposed implementation design, some GAC members raised concerns about the proposal to have all AAs serve as a "one-stop shop" for Requestors by both verifying identities and routing requests and payments for requests. Some commented that this would prove burdensome for governments. In addition, the GAC members noted that the proposed design would require Governmental AAs to assume responsibilities beyond those explicitly enumerated in Recommendation 2 of the Final Report. Instead, GAC members suggested that Governmental AAs' responsibilities be limited to verifying the identity of their users.

Countries/territories may consider using a common vendor as an accreditation authority. A vendor may be able to offer such services to many governments. It is also possible that the vendor selected to provide the Central AA services may also be able to offer AA services to governments.

3.1.2.5 Risks

The following risks relate to Governmental AA accreditation.

Risk Name	Consequences	Proposed Controls/Mitigation
Accredited governmental Requestor is in a sanctioned country.	So long as the Requestor is not on the Specially Designated Nationals and Blocked Persons (SDN) list, the data request would be placed on hold until ICANN org requests and is granted an Office of Foreign Assets (OFAC) license, which could be a lengthy and potentially costly process. ICANN org will have SSAD Terms of Use (terms may change based on final design) that address this scenario.	ICANN org could potentially investigate the possibility of obtaining an OFAC license that has a scope for all SSAD purposes for sanctioned countries. It is unknown what the likelihood of obtaining such a license may be. Governments/government agents could still approach Contracted Parties directly outside of SSAD.
Country/territory declines to designate Accreditation Authority.	Government agents would have no accreditation method that would verify their status as governmental agents, nor would they have any related benefits, such as automated disclosure in certain circumstances.	This would be considered a decision by a sovereign power that is not subject to ICANN oversight. Governments/government agents could submit disclosure requests to Contracted Parties directly (outside of SSAD) as per Implementation Guidance 2.6.
ICANN may need to de-accredit a Country/Territory-designated AA.	Should certain, limited misuses be noted, ICANN org may need to de-accredit a Governmental AA. It may take a long time to come to that decision, which carries geopolitical ramifications and questions about what to do with all users accredited by that AA.	Attempt to obtain clarification on government de-accreditation scope and impact. Develop a decision tree and warning system for Governmental AAs to reduce the risk of de-accreditation. Governments/government agents could submit disclosure requests to Contracted Parties directly (outside of SSAD) as per Implementation Guidance 2.6.

3.1.3 Legal Considerations

3.1.3.1 Legal Agreements and Related Materials

The recommended SSAD would provide several distinct functions: accreditation, including identity verification; request intake; request routing to the contracted parties; logging for each request, including details about a contracted party's response; and audits. This functionality would require interaction and cooperation between and among multiple actors, including ICANN, the Central AA, identity providers, the Central Gateway manager, as well as the SSAD Misuse Investigator and auditors. Each of these entities would be selected via RFP and

contracted by ICANN to perform their function. Legal instruments for each RFP will need to be created, and agreements between ICANN and each vendor must be negotiated and finalized during the implementation process.

In addition, the SSAD is recommended to have an undetermined number of Governmental AAs. Legal instruments setting out the expectations for this function (such as a template memorandum of understanding) will need to be created, as well.

Finally, data protection arrangements between ICANN and the Contracted Parties will need to be entered into or amended, where appropriate, and SSAD Terms of Use and other materials will be required.

Thus, the creation of legal instruments and related materials, and their negotiation with the relevant parties, will be a critical and labor-intensive aspect of the SSAD design and its implementation. This aspect of implementation will have external dependencies that will impact the timeline.

3.1.3.2 Data Protection Issues

Data, including personal data, will be transferred into, through, and out of the SSAD, including across national borders. Thus, a key legal issue to address while implementing the SSAD when drafting the agreements between and among the parties is compliance with applicable data protection laws.

The EPDP Team focused on the European Union GDPR in its consideration of data protection issues, given that this is currently the most stringent and well-known data protection regulation worldwide. However, there are many other data protection laws in existence and that could be implemented in the future, and it is possible that these could require different or additional steps for compliance for the actors within the SSAD beyond those mentioned in this ODA.

This ODA identifies specific areas relevant to GDPR compliance, but also identifies high-level data protection design principles that are relevant to data protection compliance in other jurisdictions, as well.

The SSAD must be built with “privacy by design” and “privacy by default” principles in mind. This means that data must be processed with the highest data protection principles (for example, only processing data that is necessary to be processed, storing such data only for as long as necessary, and limiting access to the data to those parties who require access to perform a specific SSAD function). As applied in the SSAD, this means that care must be taken to evaluate which SSAD operators require access to the data processed during SSAD accreditation, request submission, request evaluation, and, where applicable, disclosure of requested registration data. Data processed within the SSAD should also be encrypted, pseudonymized, and, where practicable, anonymized (such as through aggregation, especially where storage of such data over a longer period is required without the need to identify data subjects). Data processed within the SSAD must be deleted when it is no longer needed for the SSAD functions, including audits.

3.1.3.3 Implementation

Planning for agreements and related materials can be initiated early in the implementation phase. However, initial drafting of these agreements and other materials cannot be finalized

until the implementation details are well understood. Once draft agreements have been prepared, there will then be a phase of negotiation and re-drafting.

An important first step for data protection compliance is identifying the controller(s) of the processing of personal data within the SSAD under the GDPR and other applicable laws. Identification of the controller(s) is critical, because the controller is the primary entity responsible for complying with applicable data protection law requirements and is also the entity that bears the primary legal risk of the processing, including toward data subjects, as well as data protection supervisory authorities.

The identity of the controller(s) may not be clear, given the unique relationship between and among ICANN and the Contracted Parties, and uncertainties under the laws themselves. There are several broad data processing operations expected in the SSAD (each operation may also include sub-operations):

- Processing of Requestors' information for SSAD accreditation, including identity verification.
- Processing of data submitted by a Requestor in support of a request for access to registration data.
- Processing of registration data in use cases where Contracted Parties must disclose the requested data (requests that meet the criteria for "automated" disclosure).
- Processing of registration data in response to requests that require manual review by the Contracted Party.

With respect to vendors' processing of requestors' data during the accreditation process, and the processing of any personal data submitted in support of a request prior to the request being sent to the relevant Contracted Party, the identity of the controller will depend on which entity or entities determine the purposes and essential means of such processing. At this stage, it appears likely that ICANN may be a controller with respect to this processing. This will be analyzed further during the implementation phase. The role of the vendors and the contracted parties will depend on the implementation details as set out in the relevant agreements.

With respect to registration data processing by the contracted parties, the Temporary Specification for gTLD Registration Data at Appendix C identified ICANN and the Contracted Parties as controllers for the data processing activity of disclosure of nonpublic registration data to third parties. This allocation of controllership was based on applicable agreements and policies in existence at the time, leading up to the GDPR's effective date. The Temporary Specification was adopted by the Board on a temporary basis pending further policy work concerning registration data access.

Today, ICANN org believes that in circumstances where ICANN is a controller of registration data processing, it is an independent controller. This means that, in ICANN org's view, ICANN determines its own purposes and means for processing the data, and the Contracted Parties likewise determine their own purposes and means of processing registration data.

Within the SSAD, this assessment might be different. It is possible (but by no means clear) that ICANN and other parties might jointly "control" some sequence or set of processing operations of personal data within the SSAD system itself.

- If ICANN and one or more parties are joint controllers, ICANN and those parties would need to enter into joint controller agreements to comply with the GDPR.

- Controllers cannot be identified until the implementation details are solidified, because this will require assessing the facts of each data processing operation.
- The controller(s) will be identified by determining who sets both the purposes (the "why") and the means (the "how") of each data processing operation. While certain decisions concerning the means of processing can be delegated to a data processor, the controller(s) determine the essential means of processing (which and whose data will be processed, for how long, to whom access will be granted, etc.).

During the implementation phase, ICANN org could consider further consultation with data protection authorities on areas of uncertainty. A particular area of uncertainty at this stage is, in addition to issues of controllership, whether, and if so, how, the GDPR's restrictions on automated individual decision-making apply to automated disclosures and other automated processing activities within the SSAD.

Once the SSAD design has been set out in greater detail, ICANN org should, where possible, conduct and document impact assessments that may be required under applicable laws, such as Data Protection Impact Assessments under the GDPR.

- ICANN org should conduct and document transfer impact assessments (as required under GDPR and other applicable data protection laws) when specifics concerning anticipated data transfers within the SSAD are more clearly understood and to the extent that ICANN org acts as the responsible entity for conducting these assessments, as the data exporter under the GDPR.
- ICANN org must also conduct and document legitimate interests assessments where its processing as a controller is based on GDPR's legitimate interests legal basis (GDPR Art. 6(1)f), in particular if such processing will be repeated over time.
- Where assessments (data protection impact, transfer impact assessments, and/or legitimate interests) will need to be conducted at the specific accreditation or request level, ICANN org could explore the possibility of creating assessment template tools to facilitate this process.

3.1.3.4 Risks

The following are the key legal risks.

Risk Name	Consequences	Proposed Controls/Mitigation
Potential liability under applicable data protection law	Potential liability under applicable data protection laws will impact the various actors within the SSAD's ability to process personal data, including transfers of such data across borders	The SSAD must be implemented incorporating privacy by design and privacy by default. The processing of personal data must be limited to that which is necessary for the SSAD to fulfill its purpose and to facilitate compliance with data protection laws globally, which will likely evolve over time. Documenting the purposes underlying such processing and clearly mapping the data processing will enable the relevant controllers/processors (and

Risk Name	Consequences	Proposed Controls/Mitigation
		other comparable actors under applicable laws) to determine what steps must be taken to comply with laws and regulations applicable to them.
Changes in legislation and/or regulation impacting SSAD processes	New laws and/or regulations could be enacted that could require the parties operating the SSAD and Contracted Parties to take additional or different steps than those required under the GDPR, with respect to their processing of personal data. Restrictive laws could also necessitate country-specific adaptations of individual SSAD sequences or sets of processing operations (e.g., data localization requirements).	The SSAD should be implemented to comply with over-arching data protection principles, given that many if not all data protection laws and regulations have common themes. This will enable the use of the system to adapt as laws change over time.
Changes in laws/regulations impacting SSAD usage volume	Fewer requests for data access via the SSAD could occur if the contracted parties are required to publish additional registration data beyond that published today, such as under the proposed NIS2 Directive in Europe. Instances of Contracted Parties opting out of automated disclosure or denying requests for access could increase if new legislation prohibits this processing. Conversely, there could also be an increase in Contracted Parties requesting additional automated disclosures and/or disclosing more data if legislative developments reduce restrictions on data processing.	Reduced SSAD usage could result in a need for higher fees to support system operations. Monitoring of legislative developments may be needed during SSAD implementation and operation to determine if the SSAD will be impacted. ICANN President and CEO's Goal 2 for fiscal year 2022 envisions setting up "an interaction point with the community regarding legislation and legislative proposals." It is expected that potential legislative impacts to the SSAD can be evaluated as part of the implementation of this goal.
Litigation	ICANN's involvement in running the SSAD could make it a target for litigation. In addition, each	The agreements implemented for the SSAD could incorporate arbitration clauses to reduce the frequency of

Risk Name	Consequences	Proposed Controls/Mitigation
	new agreement that ICANN enters could create additional liability for ICANN. ICANN's operation of the SSAD could also make it a target of inquiries and enforcement actions from privacy regulators, government actors, and/or others who may face challenges obtaining requested data from the Contracted Parties via the SSAD.	litigation. However, it should be noted that arbitration is a lengthy and expensive process. The SSAD must be designed with data protection principles in mind. When implementing the SSAD, ICANN and the other entities operating within the SSAD must use care to meet applicable documentation and transparency requirements under applicable laws, including the GDPR. Before the SSAD is launched, all required data protection arrangements, processes, and procedures must be in place. The EPDP Phase 2 team envisioned that an SSAD risk fund could be created to help mitigate risk. The feasibility and specifics of any such fund would need to be assessed during implementation.

3.1.3.5 Issues Requiring Further Development

Economic Sanctions
ICANN must comply with the economic and trade sanctions program administered by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury. These sanctions have been imposed on certain countries, as well as individuals and entities that appear on OFAC's list of Specially Designated Nationals and Blocked Persons (the SDN list). ICANN is prohibited from providing most goods or services to residents of sanctioned countries or their governmental entities without an applicable U.S. government authorization or exemption; and ICANN generally will not seek a license to provide goods or services to an individual or entity on the SDN list. In the past, when ICANN has been requested to provide services to individuals or entities that are not SDNs, but are residents of sanctioned countries, ICANN has sought and been granted licenses as required. In any given case, however, the process to obtain such a license could be lengthy and/or OFAC could decide not to issue a requested license. Accordingly, some of the following issues may be applicable:

- ICANN org will need to conduct a review of relevant persons or entities as against the then-existing economic and trade sanctions applicable to certain countries and the SDN list maintained by OFAC (OFAC check) as needed throughout the SSAD process.
- ICANN org will need to conduct OFAC checks on any person or entity that submits an accreditation application. It is also possible that additional OFAC checks may be required when an SSAD request for data is submitted. If a person or entity is specifically

listed on the SDN list, ICANN org does not engage with such person or entity and, therefore, an accreditation or data request (or any other proposed engagement with ICANN) would be denied.

- ICANN org expects that some agreement will be needed between ICANN org and Governmental AAs. This may take the form of a memorandum of understanding (MoU) or something similar. ICANN org will need to conduct OFAC checks on the designated AA and certain employees.
- ICANN org will need to conduct OFAC checks on prospective vendors.
- If a person or entity (including a governmental entity) is in a sanctioned country, ICANN org would have to seek and be granted a license from OFAC before providing accreditation to, processing a data request for, or otherwise substantively engaging with such a person or entity. Accreditation and/or data requests, therefore, could be delayed for months (if not longer), or could be denied if an OFAC license is not granted.
- It should be noted to all Contracted Parties (possibly in the ToU) that any OFAC check conducted or any OFAC license obtained by ICANN org is applicable only to ICANN and does not extend to any Contracted Party.
- ICANN org could potentially investigate the possibility of obtaining an OFAC license that has a scope for all SSAD purposes for sanctioned countries. It is unknown what the likelihood of obtaining said license may be. Even if such a license is granted, ICANN org would still need to conduct OFAC checks as noted in the above bullet points to determine if any person or entity is on the SDN List.

Regulatory Uncertainty

There are uncertainties regarding how the GDPR applies to many aspects of the SSAD. These uncertainties include how changes in the factual circumstances of the processing would lead to different assessments under the GDPR, in particular, regarding the determination of joint controllership between ICANN and the other parties involved.

Adaptability for Evolving Regulatory Environment

The legal and regulatory environment in which the SSAD will function will continue to evolve over time. The SSAD must be able to adapt to a continually evolving environment.

3.2 Timeline

ICANN org estimates between five and six years for SSAD development and implementation, through three phases of work. Below ICANN org describes design considerations, the three phases of implementation, and outlines the associated risks to timeline achievement.

The timeline will primarily rely on the implementation work that is planned and staffed by ICANN org. The establishment of Governmental AAs can take place at any time and will not be a dependency to launch the SSAD.

Based on the complexity of the work and the resources available, ICANN org has provided two scenarios for SSAD development and implementation. Both scenarios account for two years for Phase 1: Implementation Review Team work. Where the two scenarios diverge is in the time estimated for system development: the first scenario estimates 45 months and the second 31.5 months.

See Figures 4 and 5, which illustrate the timelines.

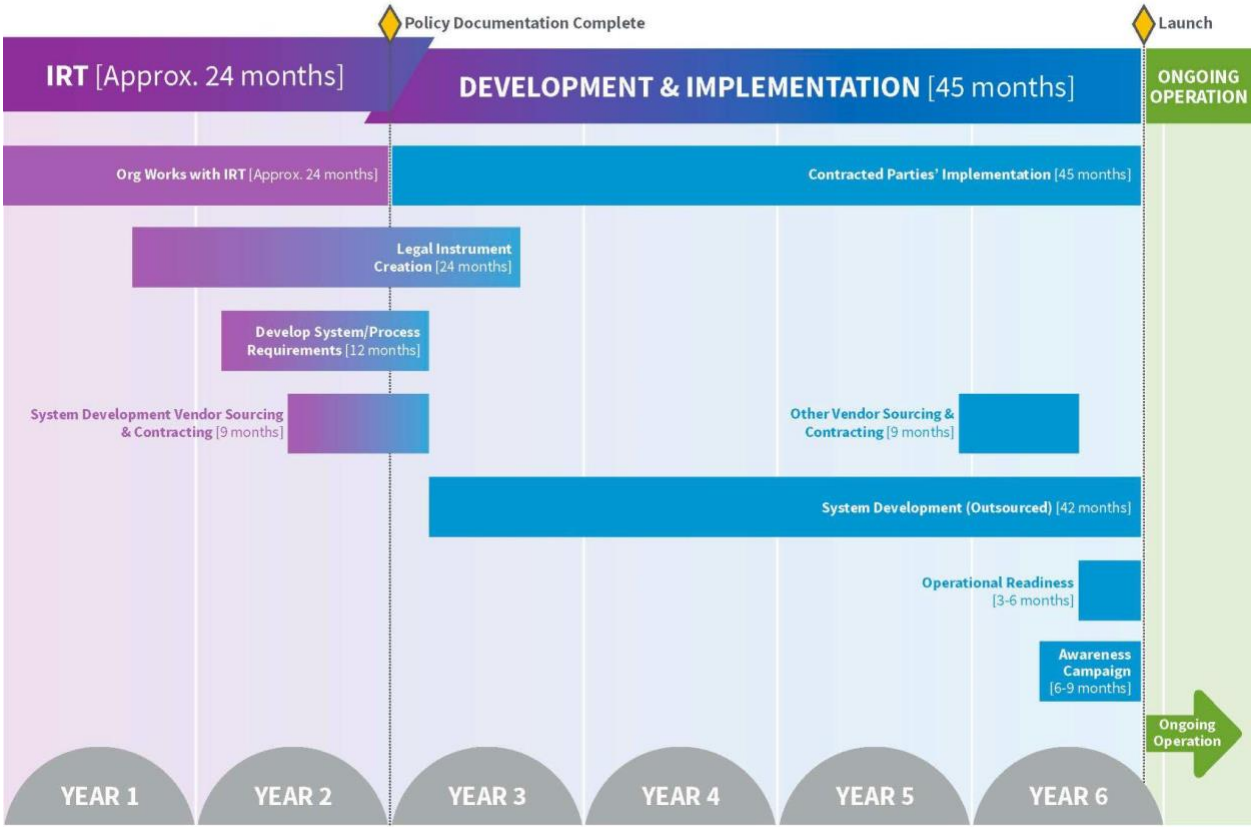

Figure 4. Timeline scenario 1 – estimated completion in six years.

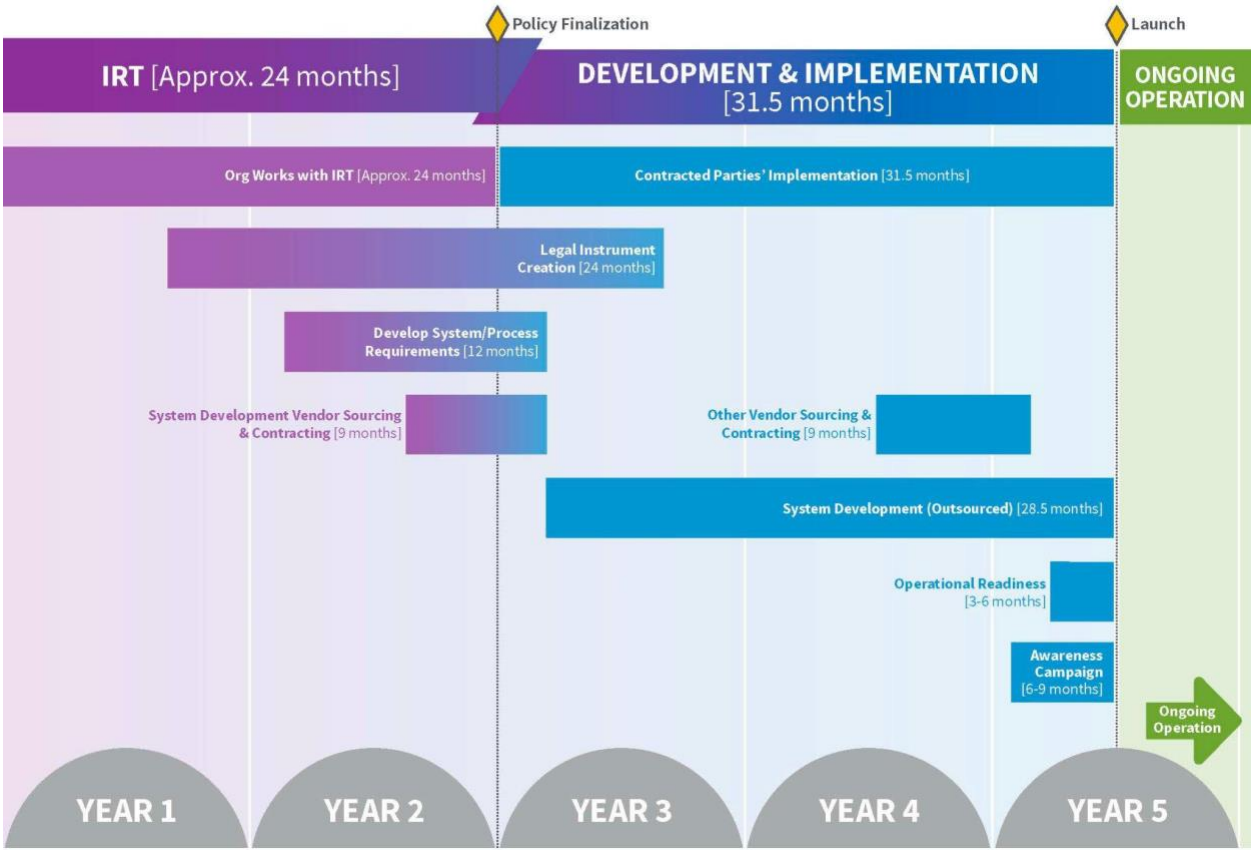

Figure 5. Timeline scenario 2 – estimated completion in five years.

ICANN org will work to complete implementation activities simultaneously as much as possible. Further details for each task can be found in other sections of the ODA. Detailed RFP information can be found in the Vendors and Third Parties section.

3.2.1 Phase 1: Implementation Review Team Work

The IRT's work as described in the Consensus Policy Implementation Framework must begin before substantial implementation work is done.

Prior to implementing the SSAD, consensus policy language must be drafted and published for community input via the Public Comment process, which lasts at least 40 days. It is difficult to predict the exact amount of time it will take to complete the drafting of consensus policy language. However, based on the policy implementation work of EPDP Phase 1, ICANN org estimates approximately 24 months for completion. The policy language will need to be updated after the Public Comment period prior to its final publication.

The following deliverables are required within the consensus policy language:

- Policy requirements for Contracted Parties.
- Policy requirements for Accreditation Authorities, Central Gateway Manager, identity provider(s), auditor(s), Requestor(s) and the SSAD Misuse Investigator.
- Contractual Compliance enforcement requirements.

Legal Instruments (Phase 1)
Vendor agreements and additional legal instruments will be developed during Phase 1. Specific tasks are as follows:

- Vendor Agreements
    - Agreements with SSAD vendors will be drafted and negotiated as vendors are selected for each function.
    - The timeline for completion of each agreement will depend on the level of complexity as well as resource factors, including how many agreements are in progress at a given time.
    - It is expected that the SSAD vendor agreements could be finalized within either of the overall timelines set out in **Figures 4 and 5** (at Timeline section 1.2); however, the timeline for negotiation of some contracts may extend beyond the period identified for vendor sourcing and contracting.

- Additional Legal Instruments
    - It is anticipated that legal instruments, such as legal assessments and data protection arrangements, will take 24 months to complete.
    - Any new or updated data protection arrangements between ICANN and the Contracted Parties would be informed by the consensus policy language developed in consultation with the IRT.
    - Implementation details will need to be solidified prior to completion of legal assessments performed per applicable data protection laws (e.g., assessments of data protection impact, legitimate interests, transfer impact).
    - Implementation details will need to be solidified prior to finalizing data protection arrangements and other legal agreements among the parties operating the SSAD.
    - Terms of Use for SSAD users will also be developed after the implementation details are well understood.

Develop System and Process Requirements (Phase 1)
This item will likely take 12 months to complete. System and process requirements will need to be developed and finalized prior to vendor sourcing.

Vendor Sourcing (Phase 1)
Based on the complexity of the systems and roles of each vendor, the entire RFP and procurement process is expected to take place at various phases of the implementation efforts, with each phase taking roughly nine months to complete.

- ICANN org will need to identify and contract with the required vendors.
- RFP planning and execution will run in parallel to policy language drafting efforts but may not be complete prior to policy language being complete.
- The design of the system will need to be more fleshed out to determine the overall complexity of the system and the length of the entire RFP process, which may vary greatly.
- The procurement process for other vendors such as auditors will take place closer to the launch of the SSAD.

3.2.2 Phase 2: System Development and Implementation

To launch the SSAD, ICANN org will need to develop various systems. The development of systems will likely begin once the policy language has been finalized. Overall system development is estimated to take between 31.5 and 45 months, or 2.5 to 3.5 years. The following items will need to be finalized prior to the SSAD launch:

- ICANN org will draft an informed timeline to develop the SSAD systems to be created and implemented once the policy language is published.
- ICANN org RDAP client will need to be enhanced to support the SSAD authentication mechanisms prior to launch.
- Development and publication of the technical interfaces for governments to integrate with will take roughly three to six months and will need to be completed prior to launch of the SSAD.
- Compliance case management capabilities, such as complaint forms within the Naming Services portal (NSp), will need to be amended prior to launch.

Contracted Parties Implementation (Phase 2)
As part of most policies, Contracted Parties are typically provided a period during which they may implement the policy requirements prior to enforcement. In the past, the period has ranged from six months to 18 months. Every effort will be made to provide as much time as possible for Contracted Parties to integrate with the SSAD.

Operational Readiness (Phase 2)
Operational readiness is a concept used to convey the activities that need to occur prior to making a service available. However, given that most functions will be outsourced to various vendors, the operational readiness activities will occur vendor by vendor. Certain milestones for readiness may be dependent upon other functions. For example, customer support for users of the SSAD will not need to be fully available until the systems enter at least a public beta test.

Awareness Campaign (Phase 2)
To promote the SSAD, communication outreach will take place for roughly six to nine months and will begin before the system is fully developed.

To implement an awareness campaign, ICANN org, its vendors, and the project leads will develop a communications plan to be run in parallel with the SSAD overall launch strategy. The communications plan will outline the approach and tactics to reach the SSAD's targeted users. This will involve ensuring the clarity of goals, target audience, and intended outcomes.

3.2.3 Phase 3: Ongoing Operations

Ongoing operations occur once the development tasks and operational readiness activities are completed, and the system is launched. Several functions will occur during operations and are generally repeatable activities in support of the system, vendors and users. Among them: Customer service will be provided to SSAD users, AA support will be provided to AAs that are integrating or have integrated with the SSAD, AA operations will be occurring with identities being verified, the system will be monitored by the CGM manager and the SSAD Misuse Investigator will be reviewing usage.

3.2.4 Risks

The following risks relate to the proposed implementation timeline.

Risk Name	Consequences	Proposed Controls/Mitigation
Delays or impasse during IRT	Possibility of diverging interpretations of the intent of policy recommendations may pose challenges within the implementation efforts. Clarifications provided from the GNSO liaison and council may not guarantee agreement of recommendation intent.	The ODP provided an opportunity to mitigate by noting the assumptions of the consensus policy recommendations and gaining clarifications where it is warranted.
Future legislation impacts on the SSAD	Future legislative developments may impact the implementation of the SSAD requiring reassessment of the system design, and updates to legal agreements or instruments, which could ultimately prolong the implementation timeline.	Monitoring of legislative developments may be needed during SSAD implementation and to determine if the SSAD will be impacted. ICANN President and CEO's goal 2 for fiscal year 2022 contemplates that the CEO will "Set up an interaction point with the community regarding legislation and legislative proposals." It is expected that potential legislative impacts to the SSAD can be evaluated as part of the implementation of this goal.
Future legislation impacts on existing agreements and policies)	Future legislation may also impact the Contracted Parties' ability to comply with existing agreements and consensus policies. This may require revisions to agreements or updates to consensus policy recommendations and/or existing consensus policies during the SSAD implementation process (if such legislation occurs during the SSAD implementation), ultimately prolonging the implementation timeline of the SSAD.	Monitoring of legislative developments may be needed to determine the effect on in-force contracts and consensus policies. ICANN President and CEO's goal 2 for fiscal year 2022 contemplates that the CEO will "Set up an interaction point with the community regarding legislation and legislative proposals." It is expected that potential legislative impacts to the SSAD can be evaluated as part of the implementation of this goal.

3.3 SSAD Operation

The SSAD operational applications are described at a high level in this section, including system inputs, outputs, and the different actors and processes involved. Based on the recommendations in the Final Report, the SSAD involves 60 processes among eight types of actors, leveraged by eight different subsystems. More detail about the SSAD business processes can be found in Appendix 1.

Two key components of SSAD operations are Accreditation Authorities and the Central Gateway (CG). AAs provide the sole system interface for Requestors, verify the identity and declarations of Requestors, receive data disclosure requests, and conduct Requestor billing operations. There are two types of AAs: one Central AA for Accreditation of non-governmental Natural and Legal Persons; and multiple Governmental AAs designated by the country/territory governments to accredit governmental and intergovernmental entities as Requestors in the SSAD.

The CG is a fully automated system responsible for routing disclosure requests to the corresponding Contracted Parties. It will also evaluate criteria for automated processing of disclosure requests. At launch, the CG will not recommend whether to approve or deny disclosure requests as described in Recommendation 5.1. A disclosure decision recommendation engine may be considered for incorporation into the system at a later time.

3.3.1 Disclosure Request Process

The nonpublic data disclosure request process is proposed to be split into three asynchronous steps:

- An Accredited Requestor submits the disclosure to the accreditation authority.
- Contracted Party reviews and makes determination about the disclosure request.
- If disclosure is approved, the Requestor queries the approved registration data from the contracted party's RDAP service.

The CG will support automated processing of disclosure requests exclusively for the four scenarios listed in Recommendation 9.4. Incorporating any other scenarios in the future would be subject to review by the GNSO Standing Committee.

Contracted Parties will have the option to request exemptions for automated processing of disclosure requests based on the requested domain name, requestor jurisdiction, or type of disclosure request. Any disclosure request that does not meet the criteria or is exempt for automated processing will be relayed to the Contracted Party for manual review.

The proposed design for manual and automated processing of disclosure requests is flexible to allow the Contracted Parties to:

- Apply their business knowledge specific to their applicable laws and jurisdiction, in their role as the sole and final authorizer of data disclosure requests.
- Ask for exemptions to automated processing of specific disclosure requests or disclosure request categories if new data protection laws or policies conflict.

The independent SSAD Misuse Investigator will monitor and handle abusive behavior in the SSAD.

The SSAD design can scale to meet reasonably anticipated, future operational changes. Examples may include modifications to the SLAs for target response times of disclosure requests, or incorporating additional scenarios for automation, with the corresponding development changes, if required by policy updates or by a GNSO standing committee per policy Recommendation 18.

3.3.2 Risks

The following risks relate to operations of the SSAD.

Risk Name	Consequences	Proposed Controls/Mitigation
Lack of consistency among different AAs' accreditation process and policies	Increased complexity for the Contracted Parties' review process of disclosure requests. Requestor identity and declarations verification may be performed differently across different accreditation authorities.	Propose Governmental AAs use the Central AA accreditation policy as a reference when defining their own accreditation policies.
Lack of controls for verification of Governmental AA to abide to their accreditation policy	Prevents ICANN org from making an informed decision when determining if a Governmental AA should be de-accredited as described in Recommendation 2.4.	Governmental AAs will be requested to provide periodic audit reports. Additionally, ICANN org will offer to cover the audit cost if the same audit process and auditor as for the Central AA are used.
Disclosure request review process not standardized among Contracted Parties	Lack of predictability in disclosure request processing outcomes.	Add the recommendation engine in the Central Gateway to provide guidance to Contracted Parties.

3.4 Systems and Tools

Since the initial SSAD implementation cost estimate provided to the ICANN Board, ICANN org has evolved the system design and the subsystem functionality. This section presents the updated estimate of the work needed to build against ICANN's evolved understanding of the requirements to implement the SSAD. ICANN org also provides cost estimates for a midpoint and high estimate, should the ICANN Board adopt the GNSO Council-approved recommendations for an SSAD for implementation.

Please note that the cost estimates in this section are only for system development. A full accounting of all SSAD implementation costs is found in the ODA section titled Costing.

3.4.1 Overview

The cost assessments are based on ICANN org's view that the quality expectations of the system stakeholders and the nature and sensitivity of their requests necessitate not only high system availability, but also a high-quality user experience to match. What follows is a detailed analysis of those costs, broken out by phases of the software development lifecycle (SDLC), beginning with conception, analysis/vendor selection, and ending with ongoing support. It is important to note that, while the estimate includes the primary functionalities envisioned in this ODA, changes in the scope and granularity of future requirements analysis could materially impact this estimate. All costs are summarized with the midpoint and high-level estimates.

The SSAD ODA estimates a midpoint cost of $11.63 million for concepting and initial deployment, followed by ongoing outsourced annual technical support and maintenance costs of $1.36 million thereafter.

SDLC Phase: Conception, Analysis/Vendor Selection
During the conception, analysis, and vendor selection phases, the E&IT team expects to provide guidance to the org and/or prospective vendors with respect to product requirements, roadmaps, scheduling/planning, vendor scoring, and technical recommendations. Refer to the Resource and Staffing section for more detail.

SDLC Phase: Implementation, User Acceptance Testing (UAT), Launch
Throughout the build, test, and launch phases, E&IT expects to provide oversight for all outsourced SSAD system implementation. Most of the implementation costs are expected to be borne by outsourced vendors. Oversight includes, among other activities, ensuring code delivery matches functional and quality expectations. The resources expected during this phase are incorporated into the estimates below based on the overall size and complexity of each system, both insourced and outsourced. Below, ICANN org provides a high-level estimate for the outsourced costs per subsystem. For insourced costs details, please refer to the Resource and Staffing section.

Because ICANN org produced an estimate for development and ongoing operations costs for the SSAD based on the EPDP Phase 2 team's draft recommendations at that time, ICANN has gone through a more extensive analysis of the final recommendations. The outcome of that analysis is presented in the following section with a high-level system design, and breakout of the major system functionality expected by the subsystems. The SSAD is expected to be composed of at least five integrated subsystems that will be either newly created or enhanced in support of SSAD requirements.

In total, the outsourced costs for initial deployment of the SSAD is estimated between $11.36 million and $16.80 million, with ongoing support costs of $1.36 million per year thereafter.

Components of the Central AA System

The Central AA will include both a web portal and API that functions as the point of entry for SSAD Requestors. The Central AA system will allow Requestors to manage their accreditation details, submit new disclosure requests by completing a form to and/or providing any required documentation, or reviewing existing requests and providing follow-up as needed. The system will also support the billing process for Requestors. This system is not expected to support the functions of the various Governmental AAs, and therefore those features have not been included in the estimate.

The Central AA is envisioned to provide support to the following business capabilities:

- Misuse management.
- Disclosure management.
- Requestor accreditation management.
- Requestor Declarations management.
- System logging and support functionality.
- User management.

These business capabilities translate to the following capabilities: workflow and case management, and document management. In addition, certain non-functional requirements are expected to be included, such as transliteration and translation, accessibility, and Universal Acceptance capabilities.

Central Accreditation Authority System		
Capability Implementation	**Level of Effort (LOE) est (hrs)**	**Cost est ($M)**
Misuse management	740 – 1000	$1.04 – $1.4
Base platform & non-functional requirements	740 – 1000	$1.04 – $1.4
Disclosure management	740 – 1000	$1.04 – $1.4
Requestor accreditation management	740 – 1000	$1.04 – $1.4
Signed assertion management	740 – 1000	$1.04 – $1.4
System logging	160 – 320	$0.22 – $0.45
System support functionality	160 – 320	$0.22 – $0.45
User management	740 – 1000	$1.04 – $1.4
Total	**4760 – 6640 hrs**	**$6.68M – $9.30M**

Figure 6. Outsourced E&IT cost estimate for implementation and deployment of the Central Accreditation Authority system.

Underlying assumptions for the estimate above include a $200/hour rate for each of the seven-person engineering team, composed of one project manager, one product manager, one architect, three software engineers, and one quality assurance engineer over the length of the initial deployment project.

Components of the CG System

The CG will include both a web portal and API that functions as the point of entry for multiple users as per the Business Process Design: Contracted Parties, AAs, SSAD Misuse Investigator, and web portal administrators.

- Contracted Parties: gTLD registries and ICANN-accredited registrars may use the web portal to access and follow up on disclosure requests directed to them, as well as other administrative processes, like reviewing or responding to their SLA reports, reporting abusive behavior by a Requestor, or updating their configuration in the system for request processing.
- Accreditation Authorities: The web portal allows the Governmental and Central Accreditation Authorities to manage the information relevant to their integration with the Central Gateway Manager and Contracted Parties, such as their point of contact or the technical details to reach their authentication endpoints.
- SSAD Misuse Investigator: The CG web portal will allow the SSAD Misuse Investigator to view and update the received misuse reports and challenges to Requestor penalization received from the Requestors through the AAs and Contracted Parties.
- Web portal administrative users: Operators of the CG web portal also perform management of the web portal; for example, to onboard/offboard an accreditation authority into SSAD.

The system supports various business capabilities with respect to disclosure management, misuse management, and SLA management, as well as various system logging and support functions. These business capabilities translate into a system that provides primarily workflow and case management, and document management.

Central Gateway System		
Capability Implementation	**LOE est (hrs)**	**Cost est ($M)**
Misuse management	740-1000	1.04 – $1.40
Base platform and non-functional requirements	320-640	$0.45 – $0.90
Disclosure management	740-1000	$1.04 – $1.40
System logging	160-320	$0.22 – $0.45
System support	160-320	$0.22 – $0.45

Central Gateway System		
SLA tracking	740-1000	1.04 – $1.40
Total	**2860 – 4280 hrs**	**$4.01M – $6.00M**

Figure 7. Outsourced E&IT cost estimate for implementation and deployment of the Central Gateway system.

***Note:** Base platform and nonfunctional requirements includes implementation of the API, data integrations, as well as support for accessibility and universal acceptance.

Underlying assumptions for the above estimates include a $200/hour rate for each of the seven-person engineering team composed of one project manager, one product manager, one architect, three software engineers, and one quality assurance engineer over the length of the initial deployment project.

Upgrading Existing ICANN Services in Support of SSAD Requirements
There are at least three existing ICANN services that are expected to receive enhancements in support of fulfilling future SSAD requirements: the ICANN org website (i.e., icann.org), ICANN RDAP client (i.e., lookup.icann.org) and the Naming Services portal (NSp) used by Contracted Parties. The technical capabilities expected to be implemented are detailed in the table below. All costs associated with updating these systems would be borne by ICANN org.

- ICANN org website: The ICANN org website is already in production but will need additional content templates for quarterly reporting on the SSAD operations, as well as forms and workflow capabilities for various misuse and compliance complaints, and data subject rights requests.
- ICANN org RDAP client: The RDAP client is currently in production, but will need to be enhanced to support the requirements of the SSAD authentication mechanism using OpenID Connect and incorporating the concepts described in "TSG01: Technical Model for Access to NonPublic Registration Data."
- Naming Services portal (NSp): The NSp is currently in production but will need to be updated to support additional enhancements related to Contractual Compliance case management capabilities.

Service / Capability	LOE est (hrs)	Cost est ($M)
ICANN org website (i.e., icann.org)		
Misuse management	40 – 80	$0.03 – $0.06
Data retention	40 – 80	$0.03 – $0.06
Reporting	40 – 80	$0.03 – $0.06

ICANN RDAP client (i.e., lookup.icann.org)		
Request registration data	160 – 320	$0.13 – $0.26
Federated authentication	160 – 320	$0.13 – $0.26
Naming Services portal (NSp)		
Case management	160 – 320	$0.59 – $0.8
Total Initial Implementation Costs	**800-1600**	**$0.88 – $1.38**

Figure 8. Estimates for upgrading existing ICANN systems in support of SSAD.

The size and complexity of the above projects are smaller in comparison to the CG and Central AA systems and therefore the expected team sizes are adjusted accordingly. For all three systems above, it is assumed that a four-person insourced engineering team would support the projects, composed of one product/project manager, one UX, one software engineer, and one quality assurance engineer. For these projects, no significant infrastructure or security effort is expected to impact cost estimates.

SDLC Phase: Post-Launch and Ongoing System Maintenance
During the final phase, the E&IT team will continue its oversight role providing technical vendor management oversight of bug fixes, minor feature development, and approved process changes. In addition, E&IT will perform periodic and ongoing audits leveraging the following technical resources on an ongoing basis throughout the life of the SSAD system. The below table details the outsourced costs associated with the ongoing maintenance of the SSAD systems. For costs associated with internal ICANN resources, please refer to the Resource and Staffing section.

Function	LOE est (hrs)	Team size	Outsourced cost est ($M)
Engineering			
Annual software maintenance and minor enhancements	1,000	1 PM 1 Arch 1 Dev 1 QA	$0.80
Infrastructure			
Annual hosting and system support			$0.48M

Security	
Ongoing security reviews and audits	$0.08M
Total Ongoing Outsourced System Support Costs	$1.36M

Figure 9. Annual SSAD support cost for ICANN E&IT and E&IT outsourced vendors.

With respect to engineering, the 1,000-hour level of effort is obtained by taking 10% of the total estimated hours for initial implementation of the CG and Central AA systems. In addition to the outsourced hours, it is expected that ICANN org personnel would provide oversight and vendor management responsibilities. Details for staff oversight are covered in the Resources and Staffing section. While it is unknown which future enhancements will be required, it is expected that the system will continue to evolve to meet the needs of SSAD stakeholders. Such enhancements, however, will be budgeted and approved prior to implementation and should be considered beyond the scope of the initial implementation of the SSAD. In addition, it should be noted that ongoing maintenance does not include all costs into perpetuity for the SSAD such as future (i.e., end of life) replatforming needs, and those events would require additional funds.

With respect to infrastructure-related ongoing costs, it should be noted that annual hosting and system support is challenging to accurately estimate prior to completion of an RFP process. For this estimate ICANN org leveraged historical systems of similar complexity, size, and capability scope. Infrastructure is estimated based on an overall system cost with respect to evaluation and oversight. This does not include any hardware or software costs to host the SSAD, nor does it include potential platform and license fees. Instead, estimated engineering costs incorporate these costs as it is assumed that custom engineering will be leveraged for these systems.

With respect to security-related costs, the ability to perform testing largely depends on the final system architecture and the extent of permissions available to security personnel. With appropriate access, security would outsource annual penetration testing and insource results analysis and review.

Summarized System Costs Estimates
The following table aggregates each of the SDLC phases with midpoint and high estimates required to implement and maintain the SSAD on an ongoing basis.

Phase	System	Midpoint Estimate	High Estimate
Conception, Analysis/Vendor Selection		See staffing	See staffing
Implementation, UAT, Launch		$11.63M	$16.80M
	Central Accreditation Authority system	*$6.68M*	*$9.30M*

	Central Gateway system	*$4.01M*	*$6.00M*
	ICANN org website	*$0.09M*	*$0.18M*
	ICANN org RDAP client (lookup.icann.org)	*$0.26M*	*$0.52M*
	Naming services portal (NSP)	*$0.59M*	*$0.80M*
Post-Launch / Ongoing System Maintenance		$1.36M	$1.36M

Figure 10. Cost estimates for technical implementation of SSAD by phase.

3.4.2 Risks

The following risks relate to the systems implementation of the SSAD.

Risk Name	Consequences	Proposed Controls/Mitigation
Significant changes to proposed architectural design due to vendor responses in RFP.	Negative impact on implementation timeline, skills required, and/or overall cost to system implementation	Determine if specific issues could be resolved via one or more pilot programs, efforts or through a research effort.

3.4.3 Issues Requiring Further Development

The ICANN Board's questions outlined in the Scoping Document included question 3.2.2., which asked, "Should ICANN org conduct a pilot program prior to launching the SSAD system?"

ICANN org notes that a pilot program can be a valuable addition to the SSAD implementation timeline, bringing additional insights into systems and tools implementation and operational readiness. A pilot program can also reduce overall risk through the use of a prototype to reduce the unknowns for specific technical and operational concerns. That said, running a pilot program would impact the cost and timeline for the SSAD launch. ICANN org could design a program to address any specific concerns the ICANN Board may have about SSAD implementation, but to be clear, the most significant unknowns – those of demand, cost sensitivity, and actual volume – would not be discoverable via a pilot program. The ODP team would welcome additional strategic guidance from the Board and community regarding scope, acceptable levels of cost, and duration of such a pilot program.

3.5 Vendors and Third Parties

ICANN org has identified the following functions that are required to operate the SSAD. The actual number of vendors will vary depending on the types of responses received via the RFP process:

- Central Gateway Manager
- Central Accreditation Authority (Central AA)
- Independent auditor
- SSAD Misuse Investigator
- System development (if different than the operator)
- Customer service operators if vendors do not offer support functions
- Public relations service provider for awareness campaigns about the SSAD prior to and post-launch

ICANN org envisions the Central AA handling the review and accreditation of requestors using its own system and policies. The Central AA may delegate the identity provider functions to one or more third parties. The contract with the Central AA should incorporate a provision for transitioning accredited users from one identity provider to another, as well as transition between vendors if a new vendor takes on the role of AA.

3.5.1 Vendor Selection

Vendor selection will be split into two stages based on logistical and logical groupings. Each of these stages are expected to last for nine months and incorporate all milestones listed below for each set of functions.

The first stage of vendor selection will include the portions of SSAD with the most complexity and effort required. This will include a selection process for the development and operation of systems related to the CG, Central AA, and potentially customer service if vendors include the service in their bids.

The second stage of vendor selection will include the remaining functions such as misuse investigation, audit, and public relations services.

Vendors will be selected via RFP where appropriate based on ICANN's procurement policy, through the standard ICANN org procurement process that is designed for transparency and vetting for conflicts of interest. It also may result in potentially lower costs because of a competitive bid process. Key, detailed milestones are listed below with a breakdown of estimated time for each.

- **RFP creation:** Four to six weeks are typically required to create RFP materials but can be longer when requirements are complex and require multiple rounds of internal review. In this case, since the requirements will come from recommendations in the Final Report and working with the IRT to determine final requirements, the RFP development process will work in parallel with applicable IRT discussions. Most RFPs include a draft contract for the requested services. Given that ICANN has not offered these services previously, contract creation will be informed by thorough requirements developed concurrently with IRT discussions. This will require substantial resources.
- **RFP issuance:** ICANN has issued RFPs for as short as three weeks, but it is advantageous to run the RFP for longer periods to attract vendors that are not aware of

the ICANN space. A two-month period would be appropriate for the scope and scale of the services and to facilitate broad participation given worldwide constraints on capacity. ICANN org intends to couple the RFP with a communications plan to reach a wide audience of potential vendors.

- **Vendor selection:** For complex services, once the RFP results are received, ICANN may request presentations from vendors. Generally, selection is completed within six weeks.
- **Negotiation and contracting:** While this work varies by contract, negotiation and contracting is typically a lengthy process. It's important to note there would be staff limitations in negotiating and revising several agreements concurrently. By splitting the overall SSAD procurement process into two phases, this helps alleviate resource contention for not only the project team, but for supporting functions in ICANN org. It would not be unreasonable to require at least 16 weeks (or more, depending on agreement complexity and the number of agreements in development) to finalize fees, legal and data protection language, and liability limits.
- **ICANN Board approval:** For commitments with a total value of or greater than $500,000, the Board Finance Committee (BFC) must review and recommend approval to the full Board. The review process for the BFC and full Board typically takes eight to 10 weeks depending upon scheduling constraints. If the ICANN Board approves the SSAD for implementation, the ODP Project Team recommends the Board pre-approve the overall implementation budget to support the system as part of the resolution to authorize the implementation of SSAD, allowing for a more expedient timeline. This would allow ICANN org to bypass individual contract approvals so long as the total remains within the overall Board-approved implementation budget.

3.5.2 Risks

The following risks relate to the vendor selection process.

Risk Name	Consequences	Proposed Controls/Mitigation
Delay in defining requirements	Delays with the vendor selection process, due to a lack of clear requirements. Requirements will result from the IRT process, but progress can be unpredictable.	ICANN org intends to iteratively develop requirements during the RFP period and leverage project management best practices to coordinate resources.
Staff resource contention	Delays with the vendor selection process, due to a lack of availability of SMEs to prepare requirements and questions to include as part of the RFP materials including draft legal documents. This risk applies to every RFP ICANN conducts.	ICANN org intends to leverage project management best practices to manage resource contention wherever possible.
High vendor costs	During the initial implementation of the system, costs may be higher because of unknown demand and volume. ICANN org has experienced this challenge in the past with the launch of	Given the unique nature of the SSAD and because the number of users and requests cannot be estimated, this risk cannot be eliminated until and unless the

Risk Name	Consequences	Proposed Controls/Mitigation
	the TMCH, in which volume could not be accurately estimated and thus created an ongoing fee obligation regardless of actual usage. This risk is related to the sustainability of the system and cost recovery risks noted in other sections.	SSAD achieves a sort of equilibrium. However, through the combination of a competitive proposal process and a plan for re-bidding after equilibrium is reached, this risk can be reduced.
Supply chain delays	Due to delays related to worldwide supply chain issues, including potential human capital/resource shortages, vendors may not bid on as many projects as they normally would. For those who do bid, there may be a significant ramp-up period until resources become available.	Communicate the RFPs well before they are published (e.g., with a blog or other methods) to provide adequate time for potential bidders to respond. Provide adequate times for bidders to bid on RFPs once published.

3.6 Resources and Staffing

Though outside vendors will perform system development and operations of the accreditation and data request processing, ICANN org personnel will serve several needed functions, as described below. ICANN org has estimated the number of full-time equivalent (FTE) hours required, based on experience.

3.6.1 Phase 1: Implementation Review Team Work

Expected duration: 24 months

Description	FTE
Product ownership	3.0
Establishment and support of IRT; alignment with GNSO/IRT	3.9
Total FTE to support this phase	6.9

Figure 11. FTE estimates for Phase 1: IRT Work.

Product ownership includes accountability and oversight of the entire product of the SSAD throughout its life. This line item encompasses project management.

Establishment and management of IRT and alignment with GNSO/IRT accounts for staff's work for various work streams, which includes:

- IRT Planning.
- Supporting the IRT's work.
- Policy language analysis and drafting.
- Public Comment Proceeding management.

- Analysis and incorporation of comments from the Public Comment Proceeding.
- Finalization and publication of the policy language.

3.6.2 Phase 2: System Development and Implementation Phase

Expected duration: 31.5 to 45 months

Description	FTE
Product ownership	3.0
Vendor sourcing and contracting	1.2
Additional legal instruments	1.7
System development	3.9
Awareness campaign	0.4
Operational readiness	0.1
Total FTE to support this phase	10.2

Figure 12. FTE estimates for Phase 2: System Development and Implementation.

Product ownership includes accountability and oversight of the entire product of the SSAD throughout its life, same as in the previous phase.

Vendor sourcing and contracting includes RFP development and management, vendor selection, negotiation, and contracting.

Additional legal instruments account for several legal instruments and related documents necessary to govern the relationship among various actors. For more information on this, refer to the Legal Considerations section.

System development encompasses oversight of and consultation on the outsourced vendor's system development, which includes:

- Weekly architectural, user experience and quality assurance reviews against ICANN org standards and guidelines.
- Periodic consulting support to ICANN org functions in support of change management processes.
- Periodic security and infrastructure audits and reviews.
- Participation during User Acceptance Testing.
- Insourced software development resources for existing ICANN system enhancements (e.g., ICANN.org, RDAP client, NSp).

Awareness campaign work includes preparation and content development; stakeholder outreach to Contracted Parties, GAC, and others; and implementation of a global awareness campaign.

Operational Readiness activities include vendor onboarding and training, contracted parties' integration with the SSAD, and onboarding of the Governmental AAs. Vendor onboarding and training.

3.6.3 Phase 3: Ongoing Operations

Description	FTE
1.3.1. Product ownership	1.0
1.3.2. Operations	3.1
Total FTE to support this phase	4.1

Figure 13. FTE estimates for Phase 3: Ongoing Operations.

Product ownership includes accountability and oversight of the entire product of the SSAD throughout its life, same as in the previous phases.

Operations encompasses the following work streams:

- Vendor management.
- System maintenance and minor enhancements.[11]
- Support of GNSO Standing Committee.
- Regular reporting.
- Management of operational costs and risk fund.
- Other org's functions work (i.e., Contractual Compliance, Global Stakeholder Services, Accounts and Services, general customer support, etc.).

3.6.4 Risks

The following risks relate to resources and staffing.

Risk Name	Consequences	Proposed Controls/Mitigation
Difficulty hiring new resources due to skills required and competitive hiring marketplace	Negative impact on implementation timeline, project, and on-going operation	Develop a comprehensive hiring strategy
Low staff retention may result in fewer resources for part or all of the project	Lack of knowledge continuity in project and/or on-going operation	Continue developing and enhancing the comprehensive employee retention program

[11] Any major enhancement (ex. the outcome from discussions with the GNSO Standing Committee, changes to the policy, or major updates to the SSAD environment) is not estimated at this time.

3.7 Costing

In this section, ICANN org presents a range of costs for system design, construction, and potential operating costs based on various project volumes for Accreditation identification requests and Requestor Declaration verifications.

3.7.1 Design and Implementation Phase

The costs to design and build the SSAD range from $20–27 million. This projection is based on the information known at the time of estimation. The range in costs is derived from the complexity and efforts to develop the system rather than anticipated volumes or system usage. The base complexity cost model was developed using the information known at the time of estimation and does not include any contingency for unknown factors during the process of design and implementation. The high complexity model includes estimates for additional efforts and costs that are not known and would become visible or known as the design and development of the system progresses. For more details regarding the technical implementation costs and range of system costs see the System and Tools section of this document.

Included in these costs are the following: development of Central AA and CG systems, ICANN org staff support, and communications-related expenses. The costs to develop the system will not be materially impacted by gaining more certainty around the projected volume of users and requests. The system design is meant to accommodate up to the volumes stated in the General Assumptions section.

Estimated Costs	Base Complexity	High Complexity
Technical Implementation of SSAD*	11,633,000	16,800,000
Communications Related	350,000	400,000
SSAD Misuse Investigator	150,000	200,000
ICANN Org Staff Support- Design	2,800,000	3,220,000
ICANN Org Staff Support- Implementation	4,400,000	5,060,000
Total	**$ 20,333,000**	**$ 27,180,000**

** See Figure 10, Cost estimates for technical implementation of SSAD by phase, for more details*

Figure 14. Estimated costs with base and high complexity.

3.7.2 Ongoing Operations

The costs to operate the system are heavily impacted by the volume of accreditation identification requests and Requestor Declaration verifications. ICANN org will be outsourcing this process and will incur costs for each accreditation verification (Natural Person Verification, User Affiliation Verification, User Representation Verification, and Requestor Declaration Verification) processed. Based on the projected volumes, the estimated cost range is $14–106 million per year to operate the SSAD. These costs include Accreditation expenses, Requestor

Declaration Verification expenses, system support and maintenance fees, user support, audit, the SSAD Misuse Investigator, and ICANN org staff support.

The table summarizes the costs under three different scenarios, a low-volume projection for each component, high-volume projection for each component, and an average or midpoint of these two projections. Projecting the volume is a challenging exercise as this system is a first for ICANN and no comparable systems exist in the market. Consequently, a lack of reliable volume projections will have a significant impact on the annual costs, most notably the Accreditation identity verification and Requestor Declaration verifications expenses. Please see Appendix 4 for information on surveys conducted among ICANN's Contracted Parties related to estimated number of requests. Appendix 5 contains a summary of responses from community members estimating demand.

Estimated Costs	Low Volume	Midpoint *(average of high and low volume scenario)*	High Volume
Accreditations/Identity Verifications	**1,200,000**	**40,600,000**	**80,000,000**
Requestor Declaration Verifications	**3,750,000**	**9,375,000**	**15,000,000**
Total Direct Expenses	**$ 4,950,000**	**$ 49,975,000**	**$ 95,000,000**
System Support External	1,088,000	1,360,000	1,564,000
User Support	1,400,000	1,750,000	2,500,000
Third Party Complaint and Audit	200,000	250,000	287,500
System Abuse Investigator	400,000	500,000	575,000
ICANN Org Staff Support	656,000	820,000	943,000
Overhead Support Costs	863,055	1,078,819	1,240,642
Annual Operating Expenses	**$ 4,767,055**	**$ 5,958,819**	**$ 7,340,142**
Development and Implementation Costs to Recover*	**$ 4,066,600**	**$ 4,066,600**	**$ 4,066,600**
Total Expenses	**$ 13,783,655**	**$ 60,000,419**	**$106,406,742**

**Recovery of Development and Implemenation costs, projecting to recovery $20.3M over 5 years, see Costing (Design and Implementation Phase) for more details on these costs*

Figure 15. Estimated expenses at low, midpoint, and high volumes.

3.8 Fee Structure

ICANN org has structured SSAD user fees so that the system development and operation costs are recovered. These costs are listed in **Figures 14 and 15**. The ODA does not include any exception to fees or fee reductions for particular groups or categories of SSAD users.

ICANN org proposes three fees: a per-Accreditation identity verification fee (Natural Person Verification, User Affiliation Verification, User Representation Verification); per-Requestor Declaration verification fee; and a per-disclosure request fee.

The cost per user will vary based on the number of accreditations needed and whether a Requestor Declaration is required for their request. Volume significantly impacts the fees that ICANN will need to charge to ensure cost recovery. Utilizing the low-volume estimate of 100,000 data requests annually, the per-accreditation identity verification fee would be $85.28, the average Requestor Declaration verification fee would be $190.00, and the per-disclosure request fee would be $39.17. Utilizing the high-volume estimate of 12,000,000 data requests annually, the per-Accreditation identity verification fee would be $21.30, the Requestor Declaration verification fee would be $160.00, and the per-disclosure request fee would be $0.43. These fees ensure cost recovery of the annual operating expenses and recovery of the costs to design and build the system. ICANN org has modeled the fees to recover the design and build expenses over a five-year period.

	Low Volume	Midpoint *(average of high and low volume scenario)*	High Volume
Accreditations/Identity Verification*	$ 85.28	$ 22.22	$ 21.30
Requestor Declaration Verification	$ 190.00	$ 166.00	$ 160.00
Disclosure Request	$ 39.17	$ 0.75	$ 0.43

**Accreditations/Identity Verification includes: Natural Person Verfication, User Affiliation Verification, User Representation Verification)*

Figure 16. Estimated user fees at low, midpoint, and high volumes.

		Low Volume	Midpoint *(average of high and low volume scenario)*	High Volume
Volume	**Users**	**25,000**	**1,512,500**	**3,000,000**
	Requestor Declaration Verifications	**25,000**	**62,500**	**100,000**
	Accreditations/Identity Verifications	**60,000**	**2,030,000**	**4,000,000**
	Disclosure Requests	**100,000**	**6,050,000**	**12,000,000**
Funding	Accreditations/Identity Verifications	5,116,828	45,112,710	85,203,371
	Disclosure Requests	3,916,828	4,512,710	5,203,371
	Requestor Declaration Verifications	4,750,000	10,375,000	16,000,000
	Total	**$ 13,783,655**	**$ 60,000,419**	**$ 106,406,742**
Expenses				
	Accreditations/Identity Verifications	1,200,000	40,600,000	80,000,000
	Requestor Declaration Verifications	3,750,000	9,375,000	15,000,000
	Total Direct Expenses	**$ 4,950,000**	**$ 49,975,000**	**$ 95,000,000**
	Annual Operating Expenses	**$ 4,767,055**	**$ 5,958,819**	**$ 7,340,142**
	Development and Implementation Costs to Recover	**$ 4,066,600**	**$ 4,066,600**	**$ 4,066,600**
	Total Annual Costs *(direct expenses +annual operating expenses + annual recovery of development implementation costs)*	**$ 13,783,655**	**$ 60,000,419**	**$ 106,406,742**
Excess *(an excess of zero confirms costs have been recovered)*				
	Total	**$ -**	**$ -**	**$ -**

Figure 17. Estimated volume of requests, funding, and expenses at low, midpoint, and high volumes.

For more information on the projected volumes, see the Assumptions section of this document, Appendix 3 – ODA Collection Methodology, Appendix 4 – Analysis of Contracted Party Questionnaire Responses, and Appendix 5 – Community Questionnaire Analysis Summary.

It is expected that neither the accreditation nor transaction fees will remain fixed for the lifetime of the SSAD. User fees may be adjusted as often as annually based on the changing number of users and requests.

Furthermore, while the operational costs of the system would be relatively fixed annually after development is completed, each system typically has a usable life. Versions of software languages eventually reach an “end of life” point where the version becomes unsupported and thus systems built on those languages must be updated. This sort of work can require significant effort and cost and may add to the overall costs that need to be recovered.

Lastly, if in the future, significant features need to be added to the SSAD based on knowledge gained through operations, from community requests and/or from input from the GNSO Standing Committee, such costs will need to be funded and would subsequently need to be recovered via Accreditation and request fees.

Fees will be directly collected from applicants. ICANN org would outsource the fee-collection function to a vendor, who would handle the transactions and collect payments on behalf of ICANN. ICANN org and the vendor will develop a process for the vendor to transfer funds to ICANN periodically.

3.8.1 Risks

The following risks relate to the estimate of costs for SSAD implementation.

Risk Name	Consequences	Proposed Controls/Mitigation
Inaccurate volume projections	Projecting the anticipated volume is a challenging exercise. Inaccurately projecting the volume could impact the ability to recover the development and operating costs.	Will revise projections as more information is learned on volume projections.
Cost estimates	Cost projections do not include costs for recommendation engine, risk mitigation costs, and future system enhancements and development.	Will revise projections when more information is learned on these topics.

3.8.2 Issues Requiring Further Development

Recommendation 14 of the Final Report is silent on whether Contracted Parties' costs should or should not be recovered through the SSAD. For the purpose of this ODP, ICANN org did not estimate the costs that may be incurred by the Contracted Parties for the development and ongoing operations of the SSAD. Considering the large number of ICANN's Contracted Parties along with their various business models, different organizational structures, varied cost bases and technical acumen, costs are expected to differ vastly. It would not be a trivial effort to determine an approach to a potential cost recovery model that includes Contracted Parties' development costs that is concurrently reasonable, fair, and equitable. If such a model can be developed, the aggregate amount of cost would have a significant impact on system costs that would then need fee support for cost recovery. This matter should be revisited in discussion with the IRT.

3.9 Risks

This section answers the ODP Scoping Document risk questions and identifies overarching risk themes. Ongoing review of the risks and appropriate updates will be made as SSAD implementation progresses, should the recommendations be adopted by the ICANN Board. It should also be noted that while best efforts have been made to identify all risks, not all risks can be reasonably foreseen until development and/or operations have begun.

3.9.1 Operational Design Phase Scoping Document Risk Questions

3.9.1.1 Would implementation of the SSAD recommendations create business, legal, reputational, or political risks for ICANN or ICANN org? (Question 3.6.1 in the ODP Scoping Document)

Implementation of the SSAD could, from a legal perspective, create potential liability for ICANN with respect to its operation of the SSAD in that relevant parties might allege ICANN has violated a law or breached ICANN's agreements (both current agreements and new agreements entered into for the purposes of implementing the SSAD). ICANN could also face an increased risk of litigation and regulatory inquiries arising out of its involvement with the SSAD, even if ICANN is ultimately not liable for any actions or omissions related to the operation of the SSAD.

3.9.1.2 Would implementation of the SSAD recommendations create any potential conflicts with the ICANN Bylaws? (Question 3.6.2 in the ODP Scoping Document)

ICANN org has not identified any conflicts with the ICANN Bylaws that would be triggered by implementation of the SSAD. Implementation of the SSAD recommendations appears to be within the scope of ICANN activities contemplated in the Bylaws.

The ICANN Bylaws, at Section 1.1(a)(i), note that implementation of policies concerning the registration of second-level domain names in generic top-level domains is central to ICANN's mission. In this role, ICANN's scope is to coordinate the development and implementation of policies developed through a bottom-up, consensus-based multistakeholder process. Annex G-1 and G-2 of the ICANN Bylaws identify the issues, policies, procedures, and principles with respect to gTLD registries and registrars that are deemed to be within ICANN's mission. These include policies regarding the "maintenance of and access to accurate and up-to-date information concerning domain name registrations."

3.9.1.3 Is there any risk that existing policy or anticipated policy changes, or ICANN contractual requirements or amendments could conflict with implementation of the SSAD recommendations? (Question 3.6.3 in the ODP Scoping Document)

As part of ICANN org's implementation of the policy recommendations from EPDP Phase 1, the org was tasked with reviewing existing policies to ensure consistency with the policy recommendations and determine if conflicts exist. ICANN org followed a similar process in assessing potential conflicts with respect to the SSAD recommendations. Following a thorough exercise by ICANN org, the ODP Project Team did not determine any conflicts with existing policies. If, however, ICANN org were to identify any conflicts during the implementation of the policy recommendations, ICANN org would notify the GNSO Council of the conflicts, per its published Consensus Policy Implementation Framework. The ICANN Board has stated that if

future consensus policy recommendations are intended to supersede current consensus policies, this must be clearly stated in the final adopted policy recommendation.[12]

3.9.1.4 What is the risk to ICANN and ICANN org if future changes in law(s) impact the implementation of the SSAD? (Question 3.6.4 in the ODP Scoping Document)

There is always a risk that laws adopted at some point in the future in one or more jurisdictions might impact ICANN org and Contracted Parties, including their ability to implement and comply with existing agreements and Consensus Policies. Because the SSAD recommendations are intended to create a standardized system for access/disclosure to nonpublic registration data, and contemplate that such disclosure must comply with any applicable law, the SSAD should be implemented in a way that the system is able to adapt to changes in law that may alter the legal standards for the disclosure of nonpublic registration data and for the processing of data within the SSAD.

As global laws on data protection evolve, there is a risk to how the SSAD may be implemented to ensure it remains in compliance with all applicable laws. To mitigate against this uncertainty, ICANN must track legislation and anticipate impacts to its policies, contracts, and systems.

3.9.1.5 Are there any recommendations where the intent is unspecified or unclear that will potentially lead to implementation challenges? (Question 3.6.5 in the ODP Scoping Document)

The SSAD ODP Project Team has engaged with the GNSO Council via the GNSO Council liaison to ensure it is accurately interpreting policy recommendations.

While those clarifications and confirmation of assumptions have proved helpful during the ODP, during the implementation phase, ICANN org will engage with an IRT to ensure implementation remains consistent with the policy recommendations. The IRT may cite disagreement with some of those assumptions during implementation.

3.9.1.6 Is there a security, stability, and resiliency concern with the implementation of the recommendations? (Question 3.6.6 in the ODP Scoping Document)

Implementation of the SSAD would result in the creation of an entirely new user base that includes information on Natural and Legal Persons. Any large, well-known system that supports a large number of users can be an attractive target to online criminals. Any breach of such data could create cascading attacks on other systems using stolen information. However, it is important to note that the SSAD will not contain any registration data.

[12] In a letter to the GNSO Council regarding EPDP Phase 1, Recommendation 7, ICANN Board Chair Maarten Botterman notes: “Absent a clear statement in new consensus policy recommendations that the new policy is intended to supersede (in whole or part) requirements in existing consensus policies, the Board’s position is that existing policy requirements will continue to stand.”

There could be several risks focused on inappropriate access to personal data processed within the SSAD, and registration data disclosed by the Contracted Parties in response to an SSAD query. Examples of inappropriate access could be a breach of databases; Requestors who are erroneously credentialed and granted access to nonpublic data; legitimately credentialed Requestors who are not authorized to see registration data but erroneously access that data.

3.9.2 Overarching Risk Themes

Each section in the Assessment includes risks specific to the area. However, several key themes emerged from those risks and are summarized below.

3.9.2.1 Complexity

The Final Report contained highly complex and interrelated requirements. The ODA contains a proposed design meant to incorporate all requirements uncovered during design discussions, along with considerations of the operational elements required to sustain the systems and vendors over time. Complex requirements have begotten a complex, multi-vendor design that result in a number of risks to delivering the design.

The most obvious risk to delivering the design is cost. Risks related to cost include a wider range of costs due to uncertainty about the effort required to design, build, and maintain systems. While the ODP team delved deeply into the requirements, there are still a number of unknowns regarding detailed elements of the system design. Solving for both the foreseeable and unknown issues may result in higher-than-expected effort from subject matter experts, software developers, quality assurance analysts and related support functions.

Duration is typically one of the single largest drivers of cost. However, time to deliver also is related to community expectations and satisfaction and is a risk factor due to the rapidly evolving regulatory landscape. With a delivery timeline ranging from approximately three to six years, it is possible that legislation will be passed in various jurisdictions that could have impacts on the timeline for delivery.

Complexity may have impacts on the security of the system. As designed, the network of systems and actors includes eight unique roles and incorporates over a thousand Contracted Parties. As a system increases its touchpoints, there is an accompanying increase in issues that can occur, including system bugs, security issues, overt failure of one or more parts of the chain, etc. Complex systems can also be more difficult and costly to maintain and offer more potential for maintenance activities and added functionality to have unintended, downstream consequences.

Lastly, complex requirements often create unique edge cases and there is a reasonable risk to uncover significant challenges during development and operation. Addressing such issues can require unexpected levels of time and effort, resulting in additional costs.

3.9.2.2 Financial Sustainability

As mentioned in the Complexity theme, the proposed design is expected to be complicated and costly. The system maintenance and other support costs are expected to continue indefinitely. Additional costs are expected throughout the SSAD's lifetime to add significant features or functions and/or to re-platform the systems to newer versions of software development environments, operating systems, etc. Some or all development costs incurred by ICANN org

are expected to be recovered, along with all operating costs, through fees assessed to the accredited users.

Mechanically, the calculation of costs for users is straightforward, but several values are unknown. ICANN org has attempted to assess potential demand and usage from those within the ICANN ecosystem. The results were ultimately inconclusive regarding the number of users who will become accredited and the volume of requests they will generate.

Further complicating the volume question is the requirement that ICANN Contracted Parties must offer reasonable access to nonpublic registration data to those who do not use the SSAD. Savvy users of registration directory services are also used to a pre-GDPR environment in which access was unlimited, free, and instant.

To create a range of potential fees, several assumptions were made about both volume numbers. However, the actual amount for either will be unknown until the capabilities are delivered and the SSAD reaches some level of stability with regard to accredited users and their associated request volume. That could take several years while the fixed costs will continue regardless of the volume of requests submitted via the SSAD.

Actual fees are meant to fund the SSAD at a cost-neutral level but can only be known after the system has been developed and enters an operating state. The proposed fees included in this assessment do not include costs for legal risks as suggested in the Final Report. Fees would be expected to vary regularly until stability is reached.

3.9.2.3 ICANN Reputation and Legitimacy of the Multistakeholder Model

The Final Report featured several minority statements reflecting dissatisfaction with the outcome of Phase 2. Community commentary has continued since adoption of the Final Report by the GNSO Council.

This ODA is solely based upon the requirements within the Final Report. Given that opinions varied on the recommendations, any implementation will carry a similar if not enhanced level of criticism. Compromise and consensus, as the hallmarks of the multistakeholder model, may also be characterized by some level of dissatisfaction. However, such dissatisfaction may be channeled into casting doubts about the effectiveness of the multistakeholder model and ICANN's effectiveness in maintaining a safe, secure, and resilient domain name system.

As noted in other themes, there is significant risk that a very expensive implementation cannot be financially sustainable. Such an outcome would result in a negative reputational impact to the ICANN model and its effectiveness.

Security for online systems that have a global presence is a challenge. From denial-of-service attacks to social engineering, the SSAD will be a target. Any actual or perceived system outage, delay in data availability, and/or data breach of any actor involved in SSAD may be attributed to failures within ICANN or ICANN org. Data breaches impact the reputation of any entity associated with the system and may impact ICANN org's reputation and pose regulatory and legal risks.

Lastly, while the SSAD acronym includes the word "standardized" it is important to note that not all aspects of the system will truly be standardized for all users. For example, some law enforcement authorities might expect that automated disclosure in response to their requests will occur in all cases, given that the Final Report, at Recommendation 9.4.1, states that "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" must be automated from the start of the SSAD. However, such automated disclosure is unlikely to occur in all cases in practice because, the Final Report also recommends that Contracted Parties may seek exemptions from automation due to local law or potentially due to too high of a burden. Furthermore, disclosure requests for different domain names submitted within a single request in the SSAD may result in many different responses due to varied approaches for Contracted Parties in different jurisdictions.

3.10 Global Public Interest Framework

The Board's scoping document included question 3.8.1: What impact, if any, do the EPDP Phase 2 recommendations have on the global public interest as evaluated using the procedural framework that was published in June 2020 and is currently being piloted? ICANN org conducted a pilot analysis using the Global Public Interest Framework to answer this question. The analysis, which is focused on the EPDP Phase 2 recommendations for the SSAD, is found in Appendix 2. As the analysis focused on the policy recommendations and not the design for the system, design and implementation analyses are not included in this section.

3.11 Contractual Compliance

ICANN org's Contractual Compliance team will play several roles in implementation of the EPDP Phase 2 recommendations for the SSAD throughout all phases. The roles include investigating complaints that Contracted Parties are failing to follow requirements and addressing any Contracted Party failure to abide by SLAs. These are explored further below.

3.11.1 Investigating Complaints

Contractual Compliance will investigate complaints from data subjects or Requestors alleging contracted parties are failing to follow the requirements in Recommendation 5.4. This recommendation specifically states the "alert mechanism is not an appeal mechanism – to contest disclosure or non-disclosure affected parties are expected to use available dispute resolution mechanisms such as courts or Data Protection Authorities…"

ICANN Contractual Compliance's role is limited to investigating complaints related to procedural failures by the Contracted Party, such as:

- Contracted Party failure to include a rationale sufficient for the Requestor to objectively understand the reasons for the decision to deny (Recommendation 5.2.3).
- Contracted Party denial of requests following a prima facie review without first seeking further information from the Requestor (Recommendation 8.6).

3.11.2 Addressing Contracted Parties' Failure to Abide by Service Level Agreements

Contractual Compliance will also be responsible for addressing a Contracted Party's failure to abide by SLAs (Recommendation 10).[13]

During the first phase of the SLA rollout, failure to comply with the SLA requirements results in a Compliance Inquiry when the Contracted Party fails to respond to an ICANN org notification regarding the SLA failure. It is only during the rollout's second phase where compliance "enforcement" is referenced immediately, in relation to failure of meeting SLAs.

As detailed in the recommendations, Priority 1 and 2 requests are intended to be made binding via an adopted Consensus Policy and, as such, may be addressed through ICANN Contractual Compliance's informal resolution stage notices due to the clear-cut requirements. However, SLAs for Priority 3 will need to be clarified during implementation, including whether they will be made binding following the IRT phase. Nevertheless, the various phase rollouts for Priority 3 request SLAs may initially result in an Inquiry.

3.11.3 Processing Complaints

Like other existing complaint types, ICANN Contractual Compliance envisions complaints or investigations related to Contracted Party requirements for SSAD may be received and processed through public-facing complaint forms that feed into the Naming Services portal (NSp) and result in individual cases. However, it may be possible to develop automation of complaints related to SLA violations as those may be triggered from internal reporting. From there, ICANN Contractual Compliance may review and process such complaints according to the process and approach described here: https://www.icann.org/resources/pages/approach-processes-2012-02-25-en

Regarding allegations of a Contracted Party violation of procedural requirements, ICANN Contractual Compliance will need to determine at time of review as to whether the matter is most appropriate for an inquiry or notice, as it will depend on the information available at the time.

Regarding the SLAs, although the Phase 1 rollout references an Inquiry, it may be determined during the implementation phase as to whether the failure to respond to an alert regarding the SLA failure warrants a notice, rather than an inquiry, in the terms considered by ICANN Contractual Compliance.

3.11.4 Implementation

The SSAD implementation phase will be important in determining specific triggers for Compliance intervention, as well as references to contractual language used as a basis for investigating complaints, and the approach for each type of complaint, such as whether the informal resolution process will begin with inquiries or escalated/notices, expected turn-around times for Contracted Parties, and criteria for resolution. Nevertheless, the implementation process will require development of template language for each scenario subject of complaint, including those that are appropriate for investigation with the Contracted Party and those that are appropriate for rejection of complaints.

[13] SLAs are described in detail in Appendix 1, Business Process Design and further explored in the Final Report. SLAs will be further developed with the IRT.

ICANN's Contractual Compliance function may require additional resources to address the additional volume of complaints that may be received in relation to the SSAD; however, this depends on the rate of complaints per number of disclosure requests. The volume of requests may not predict the volume of complaints, but ICANN org will assess whether additional resources will be required.

Furthermore, to properly establish the mechanism for receiving complaints, ICANN Contractual Compliance will require E&IT resources to develop and implement new or amended complaint forms, as well as internal functions within the NSp to receive and process such complaints. Implementation of these functions should align with the initial implementation date of the SSAD.

3.11.5 Risks

The following risks relate to the role of Contractual Compliance in implementation of the GNSO Council-approved policy recommendations related to the SSAD.

Risk Name	Consequences	Proposed Controls/Mitigation
Community dissatisfaction and demands for increased scope	Compliance intervention is limited to the scope of the SSAD recommendations and final requirements developed during the implementation phase, so there is a risk of dissatisfaction from community members if SSAD recommendations are perceived to be limited in scope. There is also potential for community pressure on ICANN org to expand the scope of Compliance intervention should the recommendations be implemented as is.	None - Compliance is unable to unilaterally expand scope beyond what is provided for in the developed policies.

3.12 Audit

The final requirements developed through the implementation phase will help determine the final scope of the audits related to SSAD usage and operations. However, as mentioned in the Vendors and Third Parties section, third-party auditors will be selected during the second phase of the vendor procurement process via RFP and as suggested, the final scope of the audits may be developed in parallel with the implementation phase.

All audits must be tailored for the purpose of assessing compliance of the auditee, 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.

In the case of AAs, an initial audit must be conducted prior to becoming fully operational. During the rest of the first and throughout the second year, the auditors would monitor and follow up on any discrepancies or outstanding issues. Subsequent audits will focus on collecting evidence based on a risk and materiality analysis, including reports of any internal audit conducted by the

AA and also collecting samples within areas of importance for the community, to ensure the internal audit works as intended.

The Central AA will be tasked with auditing identity providers, and the audit of the Central AA will reflect those audits/results. For Governmental AAs and Accredited Requestors, audits are expected to be based on a sample of requests, to ensure they are legitimate and do not violate policy. The audit cycle determines the data retention policy for the SSAD and will require all SSAD sub-service providers to preserve all operational data and system logs for a total of 18 months.

3.12.1 Scope

As previously mentioned, the full scope of audits will be finalized during the implementation phase; however, the predominant nature of the audits will be based on compliance with accreditation policies, procedures, and other requirements. These policies and requirements will primarily be reflected via system logging and made available to auditors through the Central Gateway. For instance:

- Per Recommendation 1.9.1/1.9.2, the accreditation/verification activity (such as an accreditation request) on the basis by which the decision to accredit or verify identity was made will be logged by the AA and IdP.
- Per Recommendation 15.3, the following activities should be logged by the AA: Details of incoming requests for accreditation, results of processing requests for accreditation, (e.g., issuance of the identity credential or reasons for denial) details of revocation requests, etc.
- Per Recommendation 11.7.2: The requestor "MUST, for each request for RDS data, provide representations of the corresponding purpose and lawful basis for the processing, which will be subject to auditing."

Logging requirements for identity provider(s) will be developed during the implementation phase. Nevertheless, any finalized logging requirements will be necessary for informing auditors in their compliance assessment of the parties in following procedural and policy requirements. Further logging requirements are described in the SSAD Business Design Process available in Appendix 1.

3.12.2 Results

Audit evaluation results of the AA are to be provided to ICANN org to determine if any action or remediation is required. Per Recommendation 1.4.8: "Should the Accreditation Authority be found in breach of the Accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated failure, a new Accreditation Authority must be identified or created." ICANN org will develop a framework during the IRT for managing the relationship with the Accreditation Authority, its audit results, enforcement of remediation, and criteria for replacement of an Accreditation Authority.

As it pertains to the identity providers, per Recommendation 1.6.1: "Deauthorization may occur if it has been determined that the identity provider has materially breached the conditions of its contract and failed to cure based on… ii) results of an audit or investigation by the accreditation auditor or auditor...Depending upon the nature and circumstances leading to the de-authorization of an identity provider, some or all of its outstanding credentials may be revoked or transitioned to a different identity provider." As the Accreditation Authority will be tasked with auditing the identity providers, the details of the audit results, enforcement of remediation, and

criteria for de-authorization of an identity provider will be determined during the implementation phase.

Audit evaluation results of the Accredited Requestors are to be provided to the Central AA to determine if any action is required. Per Recommendation 1.5.4: "Revocation MAY occur if the Accreditation Authority determines that the accredited individual or entity has materially breached the conditions of its accreditation and failed to cure." Additionally, per Recommendation 16.10: "Should the accredited entity or individual be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure the matter should be referred back to the Accreditation Authority and/or identity provider, if applicable, for action." ICANN org will develop requirements for how the Accreditation Authority will manage the relationship with the Accredited Requestors, its audit results, enforcement of remediation, and criteria for revocation.

3.12.3 Risks

The following risks relate to the auditing function needed for implementation of GNSO Council-approved policy recommendations related to the SSAD.

Risk Name	Consequences	Proposed Additional controls/Mitigation
Vendor lack of expertise in contracts and policies/ICANN space	Lack of familiarity could lead to delays and an increased need for staff input regarding approach and scope; otherwise, there is a risk in failing to thoroughly assess compliance.	Ensure the RFP makes reference to experience in the industry space. Request information on how the vendor will mitigate any gaps in knowledge.
Compliance with data protection regulations, and security.	Vendor will likely need to be familiar with data protection regulations; otherwise, may be subject to compliance issues. In line with data protection, security of data is of utmost importance and a failure to secure data will contribute heavily to reputational risks.	Ensure the RFP makes reference to compliance with data protection regulations, as well as effective and verifiable security measures.
Conflict of interest of vendor and Contracted Parties	Some vendor organizations may be involved in the ICANN space as Contracted Parties, which has the potential to jeopardize the integrity of the audit.	Ensure the RFP contemplates protections against any conflict of interest.
Focus on agreed upon scope	Any misunderstandings of scope may contribute to a perception the audits are not fulfilling the intended value.	Ensure there is an understanding during the RFP process regarding scope. The RFP may want to detail scope when requesting proposals to establish an up-front expectation.

Risk Name	Consequences	Proposed Additional controls/Mitigation
Vendor pricing model may change	Although contracting will initially ensure agreed upon pricing, there is potential any subsequent rounds of contracting may reflect changes to the vendors pricing model, including the potential for higher costs.	Will need to account for this possibility in the future and potentially retain information from the RFP process indicating alternative vendors should the need arise. Alternatively, ensure the budget provides for the possibility of increased cost.
Business capacity	It is unknown how many entities will be involved in the final SSAD once established; therefore, if the vendor is not capable of scaling, the audit process could be severely impacted and contribute to a perception of failure.	Ensure the RFP questions the capacity to scale, including measures to be taken by the vendor should adjustments be required in scaling.
Language capacity	As the SSAD contemplates the inclusion of multilingual content, a vendor's inability to translate or interpret various languages will hinder the audit process or halt the process entirely.	Ensure the RFP contemplates the ability to handle a wide variety of languages and scripts.

3.12.4 Issues Requiring Further Development

With reference to Recommendation 16.10, there appears to be the possibility of one-off audits pertaining to compliance with the policy requirements in addition to the details of Recommendation 1.4.8, which suggests audits of accredited entities should be conducted on a "regular basis." This will require further development, if contemplated.

Appendix 1 — SSAD Business Process Design

A1.1. Introduction

The following document describes a proposed business process design for the System for Standardized Access/Disclosure to Nonpublic gTLD Registration Data (SSAD) as per the policy recommendations included in the EPDP Phase 2 Final Report.

A1.2. Expected System Load

The proposed business design in this document is based on an assumed demand in the SSAD of three million Requestors, submitting 12 million requests per year uniformly distributed, as described in the General Assumptions section.

A1.3. Actors of SSAD

The following entity actors have been identified in the SSAD:

- **Accreditation Authority Auditor (AA Auditor):** Third-party auditing firm contracted by ICANN org to audit the Central and Government AAs to ensure compliance with their accreditation policy and other requirements.
- **Accredited Requestor**: An accredited user of the SSAD whose identity has been verified by an Accreditation Authority. Accredited Requestors are SSAD users seeking disclosure of nonpublic gTLD domain name registration data through the SSAD. Requestors identified as government entities and intergovernmental organizations may be accredited only by a Governmental AA.
- **Accredited Requestor Auditor:** Third-party auditing firm contracted by ICANN org to audit accredited users to ensure compliance with the accreditation policy and other requirements.
- **Central Accreditation Authority (Central AA):** An entity contracted by ICANN org to have the authority to accredit nongovernmental users as requestors in the SSAD. Governmental entities and intergovernmental organizations may only be accredited through the corresponding Governmental AA, and not through the Central AA.
- **Central Gateway Manager (CGM)**: An entity that will operate the Central Gateway system and/or related processes. The CGM may provide support functions for Contracted Parties and Accreditation Authorities that need to integrate with the CG. It is intended that this function be fulfilled by an outsourced vendor.
- **Contracted Party:** An entity contracted with ICANN org as a gTLD registry operator or an ICANN accredited registrar, keeper of domain name registration data.
- **Country/territory or Governmental Accreditation Authority (AA):** An entity designated by the government of a country/territory to accredit requestors that require access to nonpublic registration data for the exercise of their public policy task.
- **Data Subject:** An individual whose identifying information is being processed as part of the SSAD. This definition covers domain name contacts as well as users and operators of the SSAD components.

- **Domain Name Contact:** A Legal or Natural Person acting as contact for registered domain names, including the role of the registered name holder (registrant), technical, administrative, or other type of contact.
- **Identity Provider (IdP):** A third party subcontracted by an AA to perform one or more AA functions as described in Recommendation 1.4. In this document no functions of the Accreditation Authority refer to the identity provider (IdP), as it is up to the Accreditation Authority to decide if any functions will be delegated to an IdP. It should be noted that the term “identity provider” is used in this document as defined in the policy recommendations from the EPDP Phase 2 final report, and not in accordance with other definitions that may be found in other documents such as the OpenID Connect specifications.
- **Potential Requestor:** A user that has not yet been accredited by an accreditation authority.
- **Public:** Public Internet users.
- **RDAP Service Operator:** The entity that operates a Registration Data Access Protocol (RDAP) service for disclosing domain name registration data. This entity may be the Contracted Party itself or a third party acting as the Contracted Party’s service provider.
- **SSAD Misuse Investigator:** A function to monitor and verify potentially abusive behavior or practices by Requestors in the SSAD, as well as recommend corrective measures against abusive behavior. It is intended that this function be fulfilled by an outsourced vendor.

A1.4. Vendor Contracting

ICANN org is proposing four categories of contracts with vendors to perform the following activities:

1. A vendor to take over the role and ongoing operations of the Central AA functions, including system development and operations. The Accreditation Authority will be responsible for ensuring the proper working of their identity providers (if applicable), including audits, handling of penalizations, and management of integration with the CG, and any other actors in the SSAD.
2. A vendor for software development and operational support for the CG system.
3. A vendor to fulfill the role of the SSAD Misuse Investigator and make determinations related to monitoring and addressing reports of abusive behavior and compliance with the SSAD Terms of Use by Requestors and Accreditation Authorities.
4. One or more vendors responsible for the auditing functions of Requestors, Accreditation Authorities, and Contracted Parties in the SSAD.

A1.5. Automation of Disclosure Request Processing

As described in Recommendation 9, which details automation of SSAD processing, the system design considers support for automating the approval of data disclosure requests received that meet specific criteria. Disclosure requests that do not meet the criteria for automated processing are subject to manual review by Contracted Parties to determine the approval or denial of the data disclosure request.

Per Recommendation 9.4, only the following categories are considered to meet the criteria for mandatory automated processing of data disclosure:

- 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 and/or 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.

Disclosure requests that meet the criteria for automated processing will be considered automatically approved when they are received in the CG, except when the Contracted Party:

- Has previously notified ICANN org that it requires an exemption from automated processing.
- Has previously opted out of automated processing for the relevant domain name(s).
- Has previously opted out of automated processing for Requestors from the corresponding jurisdiction.
- The Requestor is sanctioned out of automation or is being investigated for potentially abusive behavior in SSAD.

While Recommendation 9.10 indicates that Contracted Parties may request the automated processing of certain disclosure requests beyond the categories listed in Recommendation 9.4, SSAD will not initially support such functionality. Contracted Parties may submit a request to ICANN org to include additional data fields in the disclosure request, with the purpose of allowing the Contracted Party to perform their review and process as appropriate. ICANN org will evaluate requests to include new fields to determine if they can be incorporated into the SSAD.

A1.6. Monitoring and Handling of Abusive Behavior in SSAD

ICANN org will contract a third-party entity as the SSAD Misuse Investigator to review potentially abusive behavior by Requestors in the SSAD to evaluate and determine if any sanctions or penalties are to be applied. These mitigations may take the form of rate-limiting of disclosure requests during a time, exclusion of the Requestor from automated processing of submitted requests, temporary suspension, or a definitive revocation of the Requestor's accreditation.

In addition to the behaviors listed in Recommendation 13.1.2, the following data points would also be monitored by the CGM and made available to the SSAD Misuse Investigator:

- Reports of abuse received from Contracted Parties.
- User compliance with SSAD terms of use.
- Standard operation metrics normally considered as potentially abusive in a system.

The Misuse Investigator will also be responsible to provide the redress mechanism to process requests for reconsideration received through the AA from penalized Requestors.

While Implementation Guidance 1.8.2 indicates that Contracted Parties are provided with information about sanctioned Requestors, no need was identified for doing so, since Requestors that have breached the SSAD rules will be penalized as described in the form of suspension

and/or revocation of their accreditation. Requestors using third-party providers to submit requests on their behalf can also be penalized in case of repeated breach of the SSAD rules, even if such breaches are committed by different parties acting on their behalf.

Abusive behavior by Contracted Parties in SSAD will be handled by ICANN org's Contractual Compliance function based on observed behavior and complaints received from, for example, data subjects, Accredited Requestors, or data protection authorities.

A1.7. SSAD Usage Fees

Per Recommendation 14.2, Requestors bear the primary costs of maintaining the SSAD. There are three types of fees applicable to Requestors:

1) Accreditation and re-accreditation service fees.
2) Verification and management of requestor declarations fee.
3) Disclosure request processing fees.

The fees considered are to be defined under a cost-recovery basis, all of which will be collected through the AA that accredited the user.

The Central AA is expected to charge all Requestors predetermined usage fees for providing this service. Governmental AAs may set their own fees for accreditation and Requestor declaration management (See section A.1.11.1.5) as they deem appropriate for providing their accreditation services. Disclosure request processing fees are applicable to Requestors accredited by either the Central or Governmental AAs and are to be transferred to the CGM twice a month, as applicable.

Per Recommendation 14.3, usage fees for accreditation services through the Central AA, and for processing of disclosure requests, must incorporate input of Potential Requestors in the SSAD during the implementation phase. The Consensus Policy Implementation Framework (CPIF) process will be used to account for this public consultation via public comments on the draft policy language.

A1.8. Disclosure Recommendation Engine by the Central Gateway Manager

Per Recommendation 5.1, the CGM may implement a recommendation engine as a tool for Contracted Parties to use when processing disclosure requests. Contracted Parties are not obligated to follow the CG recommendation but would be expected to provide feedback as to why they made a different decision. At launch, the proposed design does not contemplate implementing the disclosure recommendation engine as part of the CG functions, however it may be considered in the future as more operational experience with the SSAD is gained.

Providing recommendations to the Contracted Parties via the CG may help standardize and provide guidance that may be used as reference by Contracted Parties in their manual processing of disclosure requests. This in turn could be considered as beneficial to the data subjects in the form of a more predictable process for data disclosure.

If implemented, the recommendations remain only an informative reference as the determination to disclose or not remains with the Contracted Parties. Consequently, the actual

value of having the recommendations made available depends entirely on the Contracted Parties' intent to incorporate them in their review process.

A1.9. Technical Design for Data Disclosure

The proposed design for data disclosure is made with several assumptions on implementation feasibility. Further discussion with Contracted Parties and other SSAD actors is required during the implementation phase, which may result in changes to the proposed design.

The data disclosure request process will be split into three asynchronous steps:

1) The Requestor submits the data disclosure request through the Accreditation Authority, which relays it to the CG, which subsequently notifies the relevant Contracted Party.
2) The Contracted Party retrieves and reviews the data disclosure request and determines whether to approve it. The decision is communicated back to the CG and relayed to the AA and the Requestor.
3) The Requestor obtains their authenticated access of an approved disclosure request to the registration data through the Contracted Party's RDAP service.

During the implementation phase, the list of supported field subsets (as defined in RFC 8982) for RDAP partial response requests will be defined. ICANN org then will instruct all SSAD operators (i.e., Accreditation Authorities, CGM, Contracted Parties) to support them. This will ensure that only the requested data is disclosed because of an approved disclosure request in line with Recommendation 12.1.

A1.10. SSAD Interfaces

Based on the relationships among the actors, the following interfaces will be used to communicate with each other for the different business processes involved in SSAD.

A1.10.1 Central Gateway (CG) Web Portal

A web portal that functions as the point of entry for the users of the SSAD, listed below:

- **Contracted Parties:** gTLD registries and ICANN-accredited registrars may use the web portal to access and follow up on disclosure requests directed to them, as well as other administrative processes like reviewing or responding to their SLA reports, reporting abusive behavior by a Requestor, or updating their configuration in the system for request processing.
- **Accreditation Authorities:** The web portal allows the Governmental and Central Accreditation Authorities to manage the information relevant to their integration with the CGM and Contracted Parties, such as their point of contact or the technical details to reach their authentication endpoints.
- **SSAD Misuse Investigator:** The CG web portal will allow the SSAD Misuse Investigator to view and update the received abuse reports and challenges to Requestor penalization received from the Requestors through the AAs and Contracted Parties.
- **Web portal administrative users:** Operators of the CG web portal also perform management of the web portal for example to onboard/offboard an AA into SSAD.

A1.10.2 Central Gateway API

To facilitate integration and automation between the Contracted Parties and the CGM, an API will also provide most of the functions available through the CG web portal. Contracted Parties will be able to poll the CG API to check for disclosure requests that need processing, as well as

notifying of updates to specific disclosure requests. Central and Governmental Accreditation Authorities must relay the creation and updates of disclosure requests to the CG using the CG API.

It is envisioned that Contracted Parties that manage a small number of gTLDs or registrar accreditations might prefer to use the web portal. On the other hand, it is expected that Contracted Parties that have multiple gTLDs or registrar accreditations, many registrations, or simply prefer to automate their processes, will use the API instead.

A1.10.3 Central AA Web Portal

A web portal that functions as the point of entry for Requestors. The Central AA portal allows Requestors to manage their accreditation details and submit new disclosure requests by filling a form to provide any required documentation or review existing requests and provide follow up as needed. It will also support the billing process for Requestors. Notifications to Requestors related to updates on their disclosure requests will be done via email based on the information registered with the Accreditation Authority.

In the case of Governmental AAs, it is up to each country/territory to define the interface to be provided for interacting with their users.

A1.10.4 Accreditation Authority API

This API is used with two main purposes by each Accreditation Authority:

- Enable federated authentication using OpenID Connect of Accredited Requestors by the Contracted Parties in their RDAP service.[14] [15]
- Facilitating the integration and automation of different processes between the CG and the Central AA, including the receipt of updates to data disclosure requests and reports of abusive behavior tied to Accredited Requestors or specific disclosure requests.

A1.10.5 Contracted Parties' RDAP Service

Both gTLD registries and registrars are already required to operate an RDAP service. To support the SSAD, additional functionality will be required in the Contracted Parties' RDAP service, e.g., support for federated authentication using OpenID Connect[16].

A1.10.6 ICANN org Website

Quarterly reporting on the SSAD operations will be published on the ICANN org website.

A1.10.7 ICANN org Case Creation Integration API

[14] TSG01: Technical Model for Access to Nonpublic Registration Data. https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf

[15] Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect. https://datatracker.ietf.org/doc/draft-ietf-regext-rdap-openid/

[16] Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect. https://datatracker.ietf.org/doc/draft-ietf-regext-rdap-openid/.

An interface provided by ICANN org to receive notifications from the CG in order to generate Contractual Compliance cases in the Naming Services portal with the corresponding Contracted Party.

A1.10.8 RDAP Client

SSAD Requestor users will need an RDAP client to access information from the Contracted Parties' RDAP service. RDAP clients will need to support authentication using OpenID Connect.[17] It is envisioned that ICANN org's RDAP web client at https://lookup.icann.org will be updated accordingly.

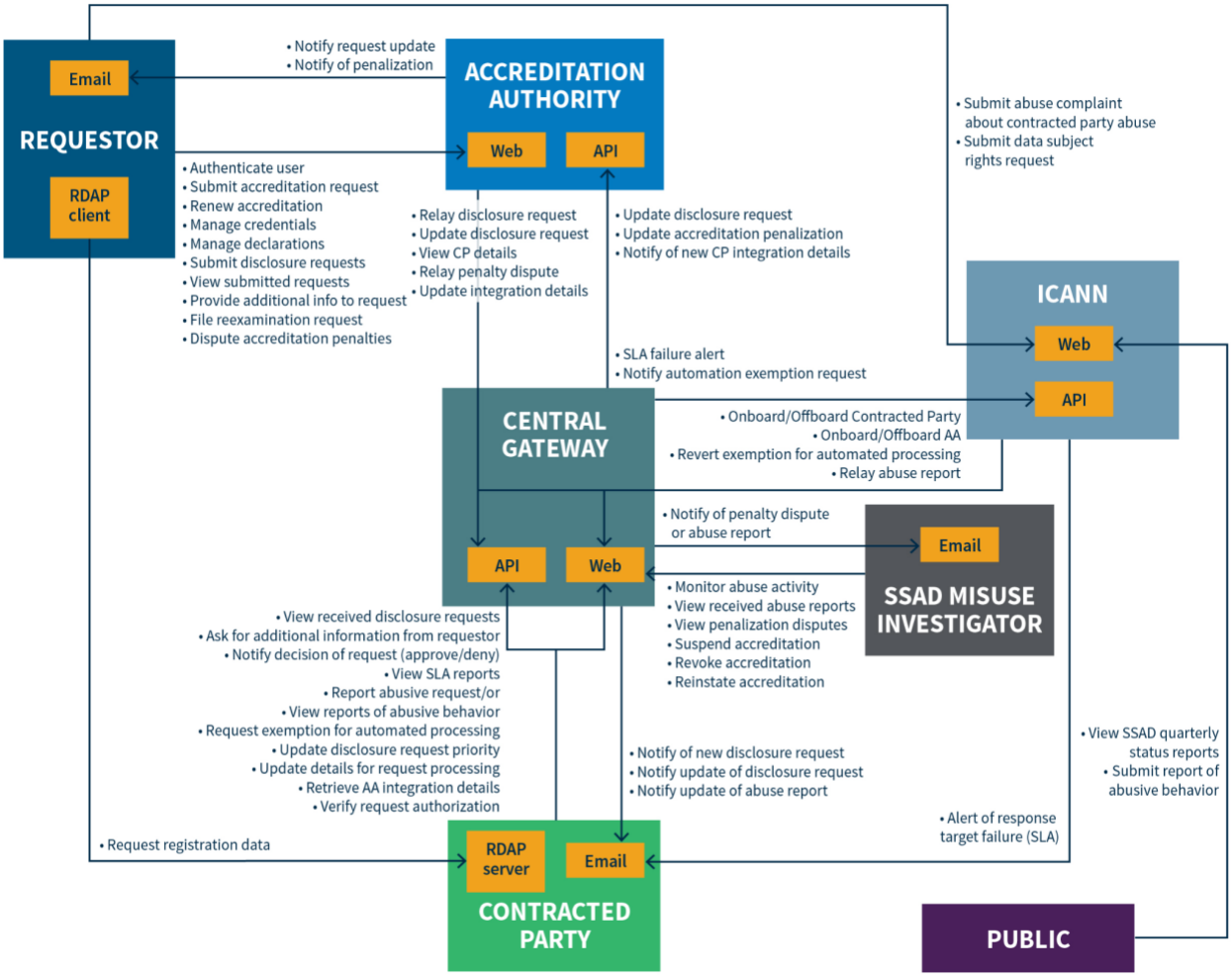

Figure A1-1. Actor relationships and interfaces.

A1.11. Business Processes

ICANN org proposes the following business processes for the design of the SSAD, listed based on the actors involved in each.

A1.11.1. Requestors with the AA

[17] Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect. https://datatracker.ietf.org/doc/draft-ietf-regext-rdap-openid/.

A1.11.1.1. Requestor Accreditation Process

Related Recommendation(s): #1

Users that seek disclosure of nonpublic domain name registration data through the SSAD must first become accredited by an AA. ICANN org will contract with a Central AA that will offer its services to non-governmental entities. Governmental entities and intergovernmental organizations may seek accreditation only with a Governmental AA.

The process begins with the Potential Requestor submitting an accreditation application to the AA to become an accredited user in accordance with the AA policy and application procedures. Accredited Requestors must acknowledge that the sharing of their personal information with the CGM and Contracted Parties may be needed as part of the process of submitting disclosure requests.

As part of the accreditation process, the application may need to be revised to correct or include additional applicant information as required by the AA and/or IdP. The process to verify the identity of Potential Requestors is described in the Operational Readiness section.

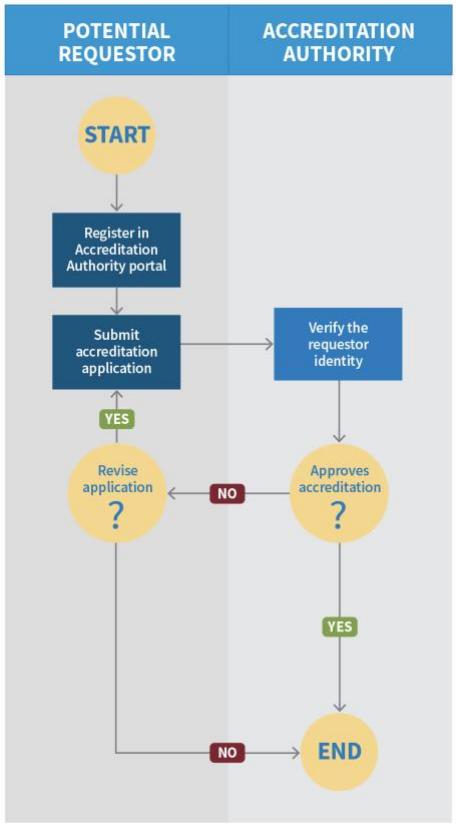

Figure A1-2. Requestor accreditation process flowchart.

A1.11.1.2. Renew Requestor Accreditation Process

Related Recommendation(s): #1.4

Based on the AA policy and accreditation process timeline, Requestors that wish to extend the validity period of their accreditation, may do so by going through a renewal process. The process to re-verify the identity of accredited users and the periodicity for renewal is described in Section 3.1.

A1.11.1.3. Process to Dispute Requestor Accreditation Penalties

Related Recommendation(s): #1.5.2, #1.5.4, #13.1.2, #13.1.3

Accredited Requestors that have been penalized as a result of abusive behavior or other breach of the SSAD Terms of Use may challenge the decision within a defined time frame, in accordance with the policy and Terms of Use. The Accreditation Authority then relays reconsideration requests to the CG.

Requestors will provide the rationale to support their appeal process for the SSAD Misuse Investigator to consider.

A1.11.1.4. Process to Manage Requestor Account Details

Related Recommendation(s): #1.3, #1.4

Accredited Requestors may login to the portal to manage the Requestor profile and account details, including any applicable credentials.

A1.11.1.5. Process to Manage Requestor Declarations

Related Recommendation(s): #1.4

Some declarations by Accredited Requestors regarding the details of an intended data disclosure request must be verified by the Accreditation Authority to be considered as valid for a predetermined time frame. Verified declarations are made available in the form of signed assertions[18] by the Accreditation Authority, which can be included by the Requestor as supporting elements when submitting a disclosure request.

At launch of the SSAD, Governmental Accreditation Authorities must support the verification of declarations for requests that may be processed automatically as described in recommendation 9.4.1 and 9.4.2. The Central Accreditation Authority will support verifying Requestor Declarations of trademark ownership. In the future, ICANN org may require AAs to support additional types of Requestor Declarations.

The AA may rely on other parties not mentioned in this document for the verification of Requestor Declarations, for example the verification of trademark holder claims, or association with a legal process or dispute.

[18] OAuth Assertion Framework. https://datatracker.ietf.org/doc/html/rfc7521

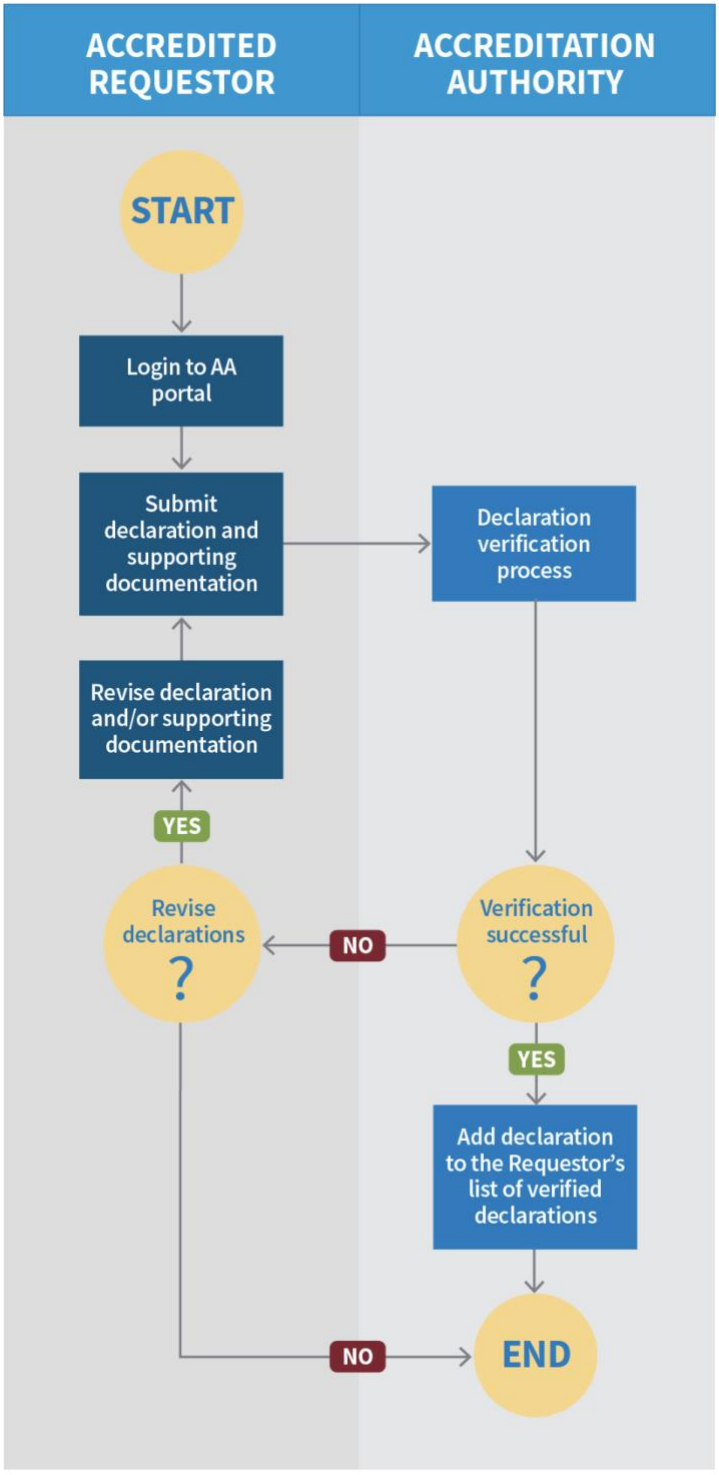

Figure A1-3. Process to manage requestor declarations.

A1.11.1.5 User Authentication Process

Related Recommendation(s): N/A

The Accreditation Authority must support authentication of Accredited Requestors to allow access to the AA portal as well as providing the Requestor authentication service for the Contracted Parties at the time of disclosure of nonpublic data.

The model for authentication of Accredited Requestors using OpenID Connect through the Accreditation Authority is described in the Technical Model for Access to Nonpublic Registration Data.[19] The AA must enable authentication as an OpenID Connect provider for the RDAP Service Operators receiving nonpublic data requests.

A1.11.1.6. Disclosure Request Submittal Process

Related Recommendation(s): #3, #4, #6, #7, #9, #13

An Accredited Requestor with valid identity credentials may submit new data disclosure requests through the AA portal. The Requestor has to pay the processing fee in advance or at the time of submitting a new disclosure request.

Once authenticated in the portal, the Requestor may create a new data disclosure request by providing all relevant information, including the list of one or more domain names involved in the request, the nonpublic registration data fields requested (by relying on predefined subsets of fields as described in RFC 8982), the purpose and legal basis of the request, the priority of the request (as defined in Recommendation 6), along with the supporting documentation and/or Requestor declarations as applicable. The Requestor may also indicate if the disclosure request should not be shared with the data subject by providing the rationale for such confidential classification. A disclosure request may only be created after the Requestor provides all required details and supporting documents.

Upon confirming that the request and documentation are valid and complete, the AA will proceed to create the disclosure request with the CG for routing to the corresponding Contracted Party for processing.

In the case of requests submitted to the Central AA, disclosure requests and supporting documentation must be submitted in the English language. Governmental AAs may support other languages only if the relevant Contracted Party has indicated support for those languages.

By default, disclosure requests will be sent to the sponsoring registrar of each domain name for processing, except when the requestor explicitly indicates the request should go to the registry operator or the registrar RDAP service is unavailable, provided that the domain name is registered using a thick registry model.

[19] TSG01: Technical Model for Access to Nonpublic Registration Data. https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf

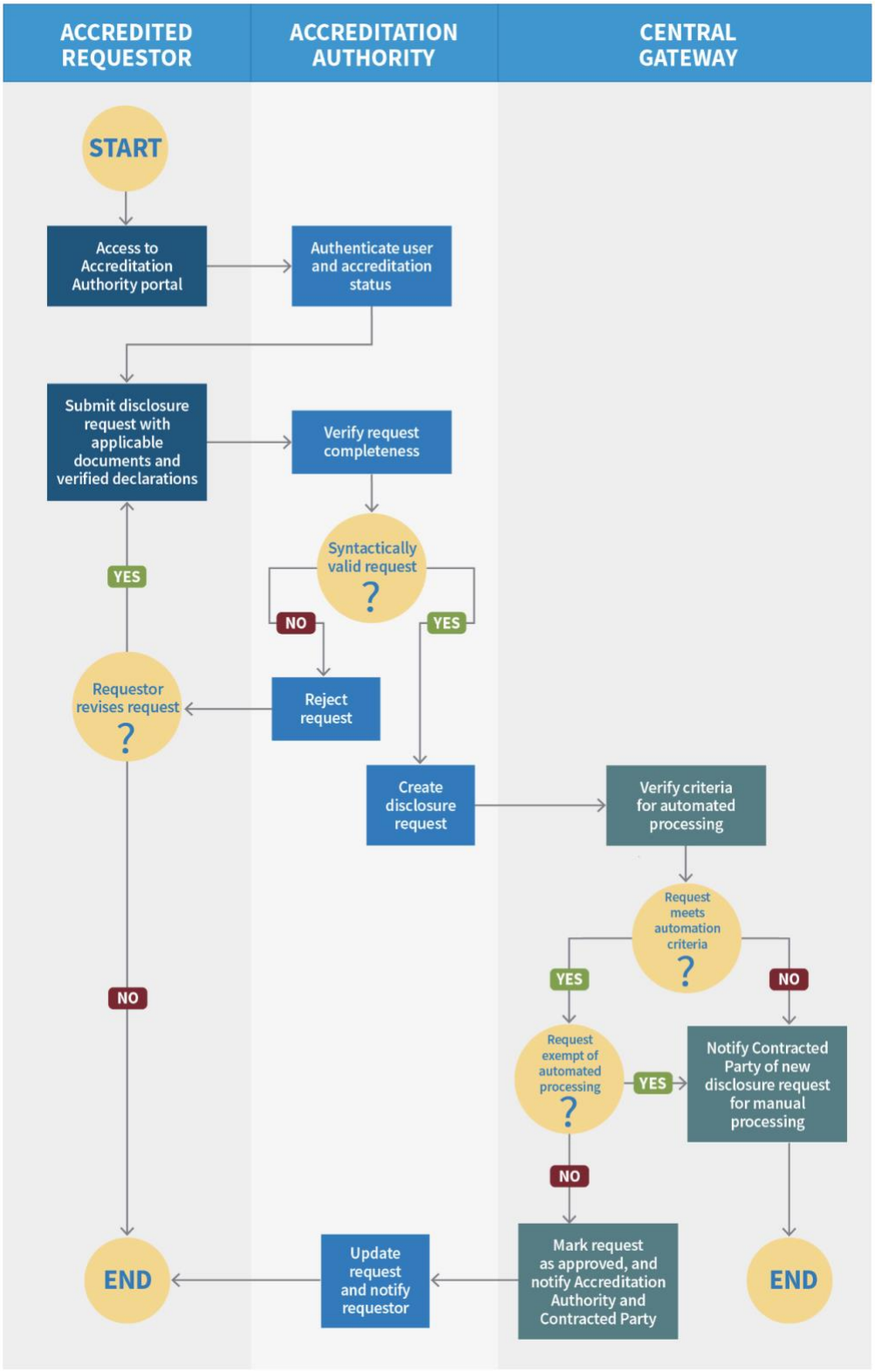

Figure A1-4. Disclosure request submittal process.

A1.11.1.6. Viewing Submitted Requests Process

Related Recommendation(s): #13.3.6

Subject to the data retention policy, requestors accredited by the Central AA will be able to login to the Central AA portal and view the details of their previously submitted data disclosure requests.

A1.11.1.7. Process to Provide Additional Information to a Disclosure Request

Related Recommendation(s): #5, #8.6

Accredited Requestors may also add a response or supporting documentation to a pending disclosure request if requested by a Contracted Party in order to complete the review of the disclosure request. After a disclosure request has been updated by the Requestor, the AA will relay the updated request to the CG.

A1.11.1.8. Request a File Reexamination Process

Related Recommendation(s): #8.4, #8.10, #8.11

If an Accredited Requestor believes that a disclosure request was improperly denied, a reexamination request may be filed through the Accreditation Authority, by providing a supporting rationale. Reexamination requests will be forwarded to the corresponding Contracted Party through the CG.

A1.11.2. Requestor/Data Subject with ICANN org

A1.11.2.1. Submit Complaint about Contracted Party's Abusive Behavior Process

Related Recommendation(s): #5.3, #5.4

Accredited Requestors and data subjects may file a complaint against a Contracted Party with ICANN org's Contractual Compliance function if they believe that systemic abuse is occurring in which disclosure requests are being denied or approved in violation of the SSAD Terms of Use.

The ICANN org's Contractual Compliance function will follow the standard process for compliance complaints to review and follow up with the Contracted Party as needed.

A1.11.2.2. Submit "Data Subject Rights" Request Process

Related Recommendation(s): #12.2.3

Accredited Requestors in the SSAD may file a "data subject rights" request with ICANN org, which would be handled by ICANN org's legal department. In the case of Domain Name Contacts identified as the affected data subject in a domain name data disclosure request, the data subject will be redirected to the corresponding Contracted Party for processing since ICANN org has no access to their data and has no way to authenticate them.

A1.11.3. Central Gateway with SSAD Misuse Investigator

A1.11.3.1. New Report of Requestor or Request Abuse or Requestor Accreditation Penalty Dispute Notification Process

Related Recommendation(s): #1.5, #13.2.1

Reports of abusive behavior in the CG will trigger a notification to the SSAD Misuse Investigator for them to review.

A1.11.4. SSAD Misuse Investigator with Central Gateway

A1.11.4.1. Monitor Requestor Abusive Behavior Process

Related Recommendation(s): #1.5, #11.1, #13.1

To identify abusive practices by Accredited Requestors in SSAD, the SSAD Misuse Investigator will monitor different metrics from the CG including reports of abuse received from Contracted Parties, general compliance with SSAD ToS, and other standard operation metrics normally considered as potentially abusive in a system.

Based on these data points the SSAD Misuse Investigator may apply different measures to Accredited Requestors demonstrating abusive practices, including:

- Limiting the allowed amount of disclosure requests by the Requestor in a given time period.
- Additional service fees based on usage.
- Temporary suspension of the Requestor.
- Revocation of the Requestor accreditation.

A1.11.4.2. Process to View Abuse Reports

Related Recommendation(s): #1.5, #13.1

The SSAD Misuse Investigator may view abuse reports through the CG as submitted by Contracted Parties and the AAs. Availability of historic data is subject to the data retention policy of the SSAD.

A1.11.4.3. Process to View Requestor Penalization Disputes

Related Recommendation(s): #1.5, #13.1

Through the CG, the Misuse Investigator may view the disputes of penalizations as submitted by Accredited Requestors. Availability of historic data is subject to the data retention policy of the SSAD.

A1.11.4.4. Revoking Requestor Accreditation Process

Related Recommendation(s): #1.5, #13.1

If an Accredited Requestor is found to breach the SSAD terms of use of the SSAD, or to no longer meet the requirements for accreditation, a revocation of the accreditation may be triggered.

After a user accreditation has been revoked, declarations and identity credentials associated with the Requestor will no longer be valid in SSAD. The Requestor must go through the accreditation process again to be able to submit new disclosure requests through the SSAD. However, the causes for any past revocation must be considered as part of the verifications performed during the accreditation process.

A1.11.4.5. Suspension of Requestor Accreditation Process

Related Recommendation(s): #1.5, #6.4, #13.1.3

As part of the graduated sanctions against abusive user behavior in SSAD, in addition to terminating accreditation of a Requestor, limited suspensions may also be imposed depending on the type of abuse.

The suspension of a user accreditation may limit the number of requests submitted by said user, prevent from submitting disclosure requests flagged for urgent processing, or prevent submitting any new disclosure requests altogether for limited periods of time. A suspended accreditation is not considered to be revoked and the suspended status may end after a period or be lifted by the Misuse Investigator without the need for the user to go through the accreditation process again.

A1.11.4.6. Process to Reinstate Requestor Accreditation

Related Recommendation(s): #1.5.2

As the outcome of the appeals process by a Requestor to dispute their accreditation suspension or revocation, the Misuse Investigator may determine that the user accreditation is reinstated. Reinstating a user accreditation effectively removes any penalties previously imposed by the suspension or revocation.

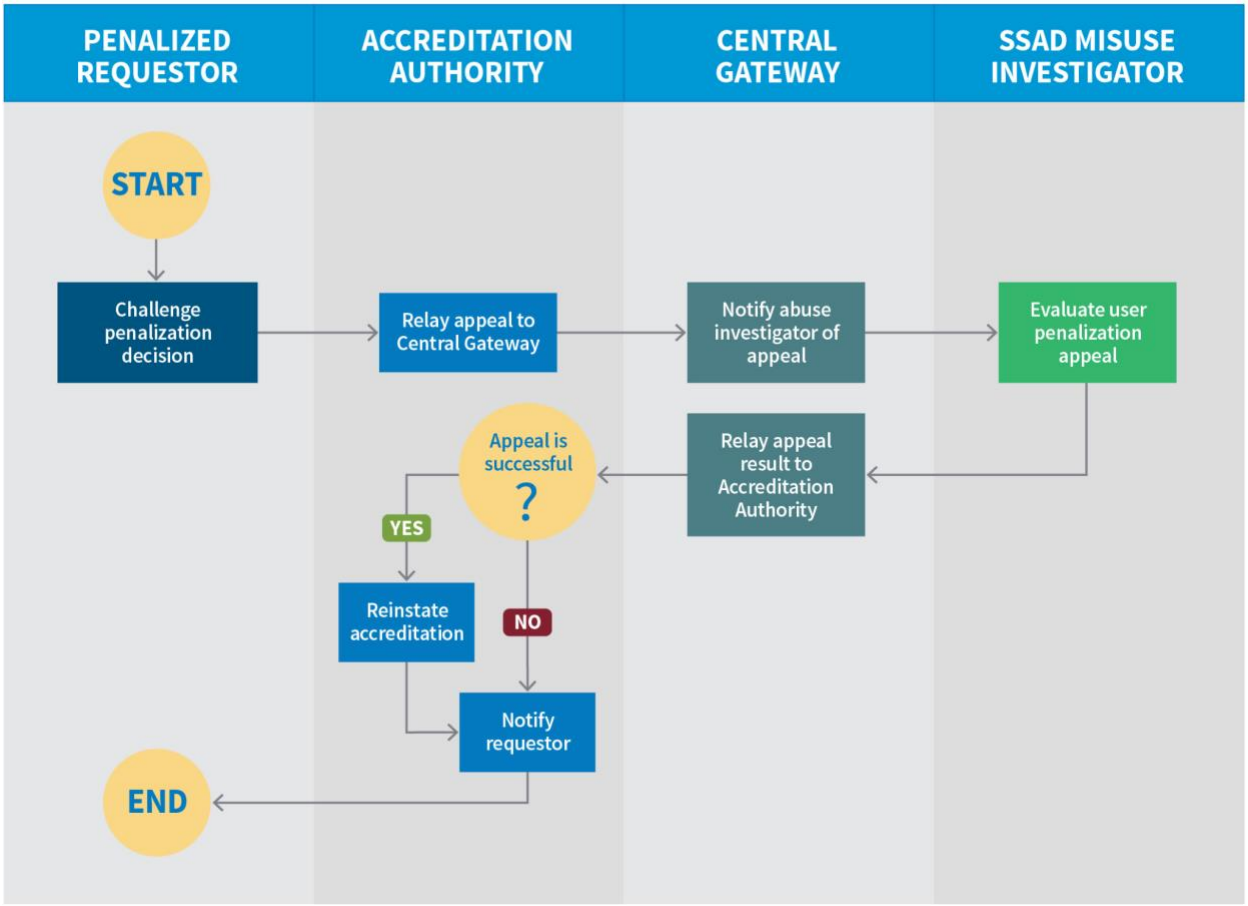

Figure A1-5. Requestor dispute of accreditation penalizations process.

A1.11.5 Accreditation Authority with CGM

The processes in this section refer to both the Central Accreditation Authority and Governmental Accreditation Authorities.

A1.11.5.1. Relay Disclosure Request Process

Related Recommendation(s): #3, #4, #6, #7, #9, #13

Disclosure requests submitted by Accredited Requestors that the Accreditation Authority has verified to be valid and complete will be relayed to the CGM.

The identity of the Requestor and verified declarations are provided to the CG by the Accreditation Authority encoded as claims in a signed JSON web token (JWT) as described in section 5 of the OpenID Connect Core specification.[20]

A1.11.5.2. Update Disclosure Request Process

Related Recommendation(s): #5, #8.6

[20] OpenID Connect Core. https://openid.net/specs/openid-connect-core-1_0.html

- All updates made by Accredited Requestors to existing disclosure requests submitted by Accredited Requestors will be relayed to the CGM.

A1.11.5.3. Relay Accredited Requestor Penalization Dispute Process

Related Recommendation(s): #1.5

Disputes to penalizations to Accredited Requestors that the Accreditation Authority has received will be relayed to the CG.

A1.11.5.4. Process to Submit Report of Requestor Abusive Behavior

Related Recommendation(s): #13.1.1
If the Accreditation Authority detects any pattern of abusive behavior from Requestors, it may submit the corresponding report with the supporting rationale to the CG.

A1.11.5.5. Funds Transfer for Operational Costs Process

Related Recommendation(s): #14.2, #14.4

The corresponding funds for accreditation and submitted disclosure requests as defined in the Accreditation Authority policy and billing structure must be transferred twice per month to the CG.

A1.11.5.6. Update SSAD Integration Details Process

Related Recommendation(s): N/A

As part of the onboarding information of the Accreditation Authorities in the CG, the Accreditation Authority may manage the configuration of their integrations with the CG portal.

Configuration of the Accreditation Authorities include:

- Points of contact of the Accreditation Authority.
- Managing authentication credentials to the CG portal and API.
- Federated authentication details.

If the Accreditation Authority delegates any functions to an identity provider related to integration, any integration information must be maintained by the Accreditation Authority as applicable.

A1.11.5.7. View Contracted Party Integration Details Process

Related Recommendation(s): N/A

Accreditation Authorities may view the integration details provided by each Contracted Party related to the processing of disclosure requests, for example, the list of supported languages.

A1.11.6. CGM With Contracted Parties

A1.11.6.1. Notify Contracted Party of New Disclosure Request Process

Related Recommendation(s): #3, #4, #5.1, #6, #7, #9, #13

The CG will notify of all disclosure requests received from the Central AA or a Governmental AA via email. Additionally, the notification will be available as a poll message to Contracted Parties through the CG API.

The CG's notification will indicate if the conditions for automated processing and disclosure are met or not.

A1.11.6.2. Notify of Disclosure Request Update Process

Related Recommendation(s): #5, #8.6

The CG will notify the relevant Contracted Party of all updates received on pending disclosure requests received from the Central AA or a Governmental AA via email and made available as poll messages through the CG API.

A1.11.6.3. Notify of Update to Abuse Report Process

Related Recommendation(s): #13.1

The CG will notify the relevant Contracted Party of all updates received from the Misuse Investigator on reports of abusive behavior submitted by the Contracted Party. The notification will be sent via email and made available as poll messages through the CG API.

A1.11.7. ICANN org with Contracted Parties

A1.11.7.1. Alert of Response Target Failure Process

Related Recommendation(s): #10.7, #10.10

Whenever a Contracted Party fails to meet the disclosure response target as defined in the service level agreements for processing data disclosure requests, ICANN org Contractual Compliance will alert the Contracted Party accordingly.

As indicated in Recommendation 10.14, response and compliance targets are expected to be reviewed by the GNSO Standing Committee.

A1.11.8. Contracted Parties to CGM

A1.11.8.1. View Received Disclosure Requests Process

Related Recommendation(s): #13.3.6

Subject to the data retention policy to be defined, Contracted Parties may access the CG portal to view received disclosure requests. This process may also be done using the CG API.

A1.11.8.2. Request Process for Additional Information on Received Disclosure Request

Related Recommendation(s): #8.6, #8.14

A Contracted Party that determines that a disclosure request is not valid (e.g. it does not provide sufficient grounds for a substantive review) may respond to such request with an intent to deny unless further information is provided by the requestor. This process is available to the Contracted Parties through the CG portal and API which will trigger updating the request with the corresponding AA.

A1.11.8.3. Review Disclosure Request Process

Related Recommendation(s): #5.2, #12, #13.1.3

To process a received disclosure request, a Contracted Party must first retrieve the details of the request from the CG through the web portal or the API, which will allow the Contracted Party to determine if the request has been flagged for automated processing.

As part of the manual review, the Contracted Party must process data in compliance with applicable law considering the jurisdiction of the Requestor and the data subjects. In the case of disclosure requests based on consent by the registered name holder, the Contracted Party must verify that such consent was provided.

Once the request has been processed, the Contracted Party must report the request outcome to the CGM. For the purposes of automating future requests on the same domain name(s), the Contracted Party will have the option to indicate to the CG if the disclosure request has been approved because the domain name registration data does not include any personal data.

If the request is approved, access to the nonpublic registration data will be granted to the Requestor for a limited amount of time (to be defined during the implementation phase), the notification to the Requestor will include the instructions to retrieve the data directly from the Contracted Party's RDAP service.

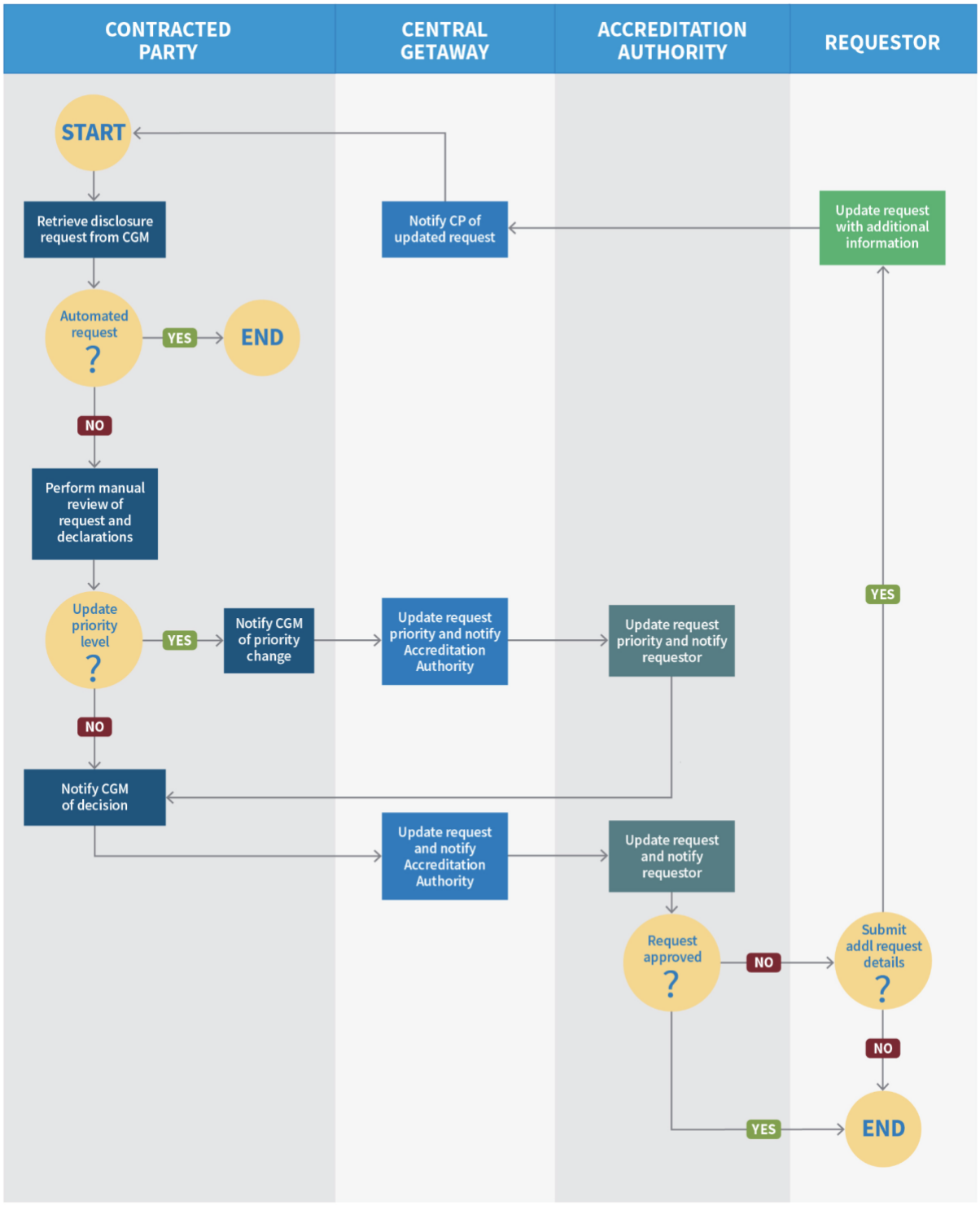

Figure A1-6. Disclosure request review process.

A1.11.8.4. Process to View SLA Reports

Related Recommendation(s): #10

Based on the agreed-upon SLAs, Contracted Parties always have access to view their SLA measurements using the CG portal and API.

A1.11.8.5. Report Perceived Abusive Requestors/Requests Process

Related Recommendation(s): #13.2.1

Contracted Parties will have the option to submit a report of abuse from a specific Requestor or disclosure request using the CG portal and API. Received reports will be relayed to the SSAD Misuse Investigator for review.

When a request is reported as abusive, the Contracted Party will be permitted to delay the request response, without impact to the response target measurements, until a determination on the abuse report has been made.

A1.11.8.6. Notify Exemption of Automated Processing of Disclosure Request Process

Related Recommendation(s): #9.4, #12.3

Contracted Parties may notify the CG whenever disclosure requests corresponding to specific domain names or Requestor jurisdictions may not be processed automatically despite meeting the criteria for automated processing, for example due to an objection from the data subject, or because the registration data has changed for a domain name previously flagged for automated processing for not including personal data as described in recommendation 9.4.4.

A1.11.8.7. Request Exemption Process for Automated Processing of Disclosure Request Category

Related Recommendation(s): #9.4, #9.5, #9.6, #9.7, #9.8, #12

If a Contracted Party determines that it is not legally permissible to process disclosure decisions meeting the criteria for automated processing, or brings a significant risk, the Contracted Party must request an exemption for automated processing of the relevant category of disclosure requests, including all supporting documentation. This exemption may be requested through the CG portal.

Upon submitting this request subsequent disclosure requests under the identified category will no longer be considered by the CG to meet the criteria for automated processing.

A1.11.8.8. Update Disclosure Request Priority Process

Related Recommendation(s): #6.3

If during the manual review of a disclosure request the Contracted Party determines that a request priority level is inaccurate, the Contracted Party may update the priority level through the CG portal or API.

A1.11.8.9. Update Details for Request Processing

Related Recommendation(s): #9.10

As part of the onboarding information of Contracted Parties in the CG, the Contracted Party may manage the configuration for processing their disclosure requests with the CG portal.

Configuration of the Contracted Parties includes:

- Defining points of contact for the Contracted Party.
- Managing authentication credentials to the CG portal and API.
- Supported languages for disclosure request details and documentation.

A1.11.8.9. Retrieve AA Integration Details Process

Related Recommendation(s): N/A

Contracted Parties may view the AAs' integration details for federated authentication of Requestors through the CG portal.

A1.11.9. Contracted Parties to ICANN org

A1.11.9.1. Respond to SLA Failure Alert/Notice Process

Related Recommendation(s): #10.8, 10.9, 10.10

For all received alerts of response target failures based on the defined SLAs, Contracted Parties must provide a response via email including the rationale as to why the response target was not met.

A1.11.10. Requestor to RDAP Service Operator

A1.11.10.1. Process to Obtain Data Related to an Approved Request

Related Recommendation(s): #12, #13.1.3

The actual disclosure of nonpublic registration data for approved disclosure requests occurs directly between the Requestor and the Contracted Party through the latter's RDAP service. The authentication process proposed to be supported by the RDAP servers uses federated authentication.[21] [22]

The data disclosure process starts when the Requestor of an approved disclosure request sends the request to the Contracted Party's RDAP service, which redirects the user to the Accreditation Authority as determined by the Requestor identifier for authentication. After authentication is successful, the RDAP Service Operator sends a request to the CG API to

[21] TSG01: Technical Model for Access to Nonpublic Registration Data. https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf

[22] Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect. https://datatracker.ietf.org/doc/draft-ietf-regext-rdap-openid/

verify that the request has been authorized for the authenticated user and the requested nonpublic data.

If authorization is verified successfully, the requestor will be redirected back to the RDAP service which notifies of the disclosure to both the data subject and the CGM and proceeds to provide the RDAP response corresponding to the requested domain registration data. As part of the data disclosure process, contracted parties may be required to send a notification to the impacted data subject(s) indicating their data has been processed and disclosed.

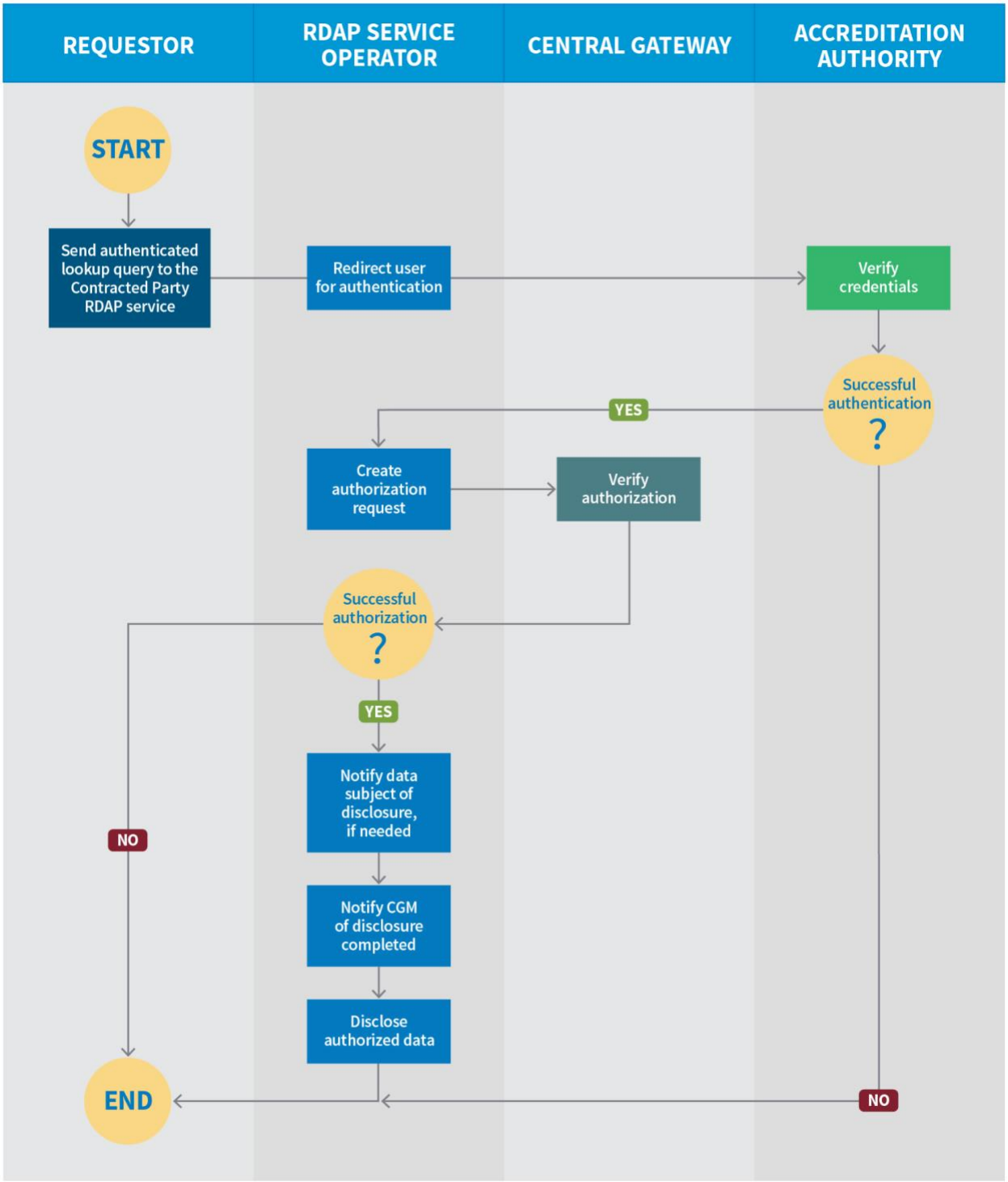

Figure A1-7. Registration data disclosure process.

A1.11.11. RDAP Service Operator to CGM

A1.11.11.1 Verify Request Authorization Process

Related Recommendation(s): N/A

When processing an RDAP query from an Accredited Requestor that has been authenticated by the Accreditation Authority, the RDAP Service Operator sends the RDAP request along with the received ID token and optional access token, to the CG API to verify that the disclosure of the requested nonpublic data has been approved for the Requestor. The tokens are validated as described in Sections 3.1.3.7 and 3.1.3.8 of the OpenID Connect specification[23], and the identity attributes (known as "claims" in OAuth 2.0) are retrieved from the ID token.

The CG API response indicates the result of the authorization processing.

A1.11.12. Central AA to Requestor

A1.11.12.1. Process to Notify Requestor of Request Processing Updates

Related Recommendation(s): #8.6, #12

Updates to data disclosure requests received by the Accreditation Authority will be communicated to the Requestor via email, including the determination of the disclosure request by the Contracted Party, and requests for further information.

A1.11.13. CGM to Central or Governmental AA

A1.11.13.1. Update Disclosure Request Process

Related Recommendation(s): N/A

All updates by Contracted Parties to existing disclosure requests submitted by Accredited Requestors will be relayed to the corresponding Accreditation Authority where the relevant Requestor will be notified of the updates and be able to see them.

A1.11.13.2. Process to Update Accreditation Penalization

Related Recommendation(s): #1.5, #6.4, #13.1

The CG will relay to the AA all the determinations made by the Misuse Investigator related to penalization of Accredited Requestors. These determinations include suspension, revocation, or reinstatement of an accreditation.

A1.11.13.3. Process to Notify of New CP Integration Details

Related Recommendation(s): N/A

The CG will notify the Accreditation Authorities when Contracted Parties update their details for request processing, for example when the Contracted Party updates supported languages.

A1.11.14. ICANN org to CGM

[23] OpenID Connect Core. https://openid.net/specs/openid-connect-core-1_0.html

A1.11.14.1. Onboarding of Contracted Party Process
Related Recommendation(s): N/A

When a new Contracted Party is created (e.g. a gTLD is delegated or a new registrar is accredited with ICANN) ICANN org must onboard the Contracted Party to allow them to use the CG system.

A1.11.14.2. Offboard Contracted Party Process
Related Recommendation(s): N/A

The ICANN org must offboard the Contracted Party from the CG when a TLD gets revoked from the root, or a registrar accreditation is terminated.

A1.11.14.3. Revert Request Process for Exemption of Automated Processing
Related Recommendation(s): #9.5

The ICANN org may revert exemption of automated processing of a disclosure request category for a Contracted Party through the CG portal. Reverting this exemption will cause the CG to consider disclosure requests under this category to meet the criteria for automated processing.

A1.11.14.4. Onboarding Process for Governmental AA
Related Recommendation(s): #2

The ICANN org will onboard to the CG any entities that have been designated to become accredited as Governmental AAs in SSAD as described in Section 3.1.2 Country/Territory/Government Accreditation.

A1.11.14.5. Offboarding Process for Governmental AA
Related Recommendation(s): #2.4

The ICANN org will offboard from the CG any entity that has been de-accredited as a Governmental AA from the SSAD, as described in Section 3.1.2 Country/Territory/Government Accreditation.

A1.11.14.6. Relay Abuse Report Process
Related Recommendation(s): N/A

Reports of abuse submitted to the ICANN org will be relayed to the CG.

A1.11.15. CGM to ICANN org

A1.11.15.1. Process to Send SLA Failure Alert
Related Recommendation(s): #10.7

Failure of Contracted Parties to meet response targets within the agreed SLAs for data disclosure processing will cause an alert to the ICANN org through an integration API to automate case creation with the corresponding Contracted Party.

A1.11.15.2. Notification Process of New Exemption Request by Contracted Party of Automated Processing

Related Recommendation(s): #9.5, #9.6

The CG sends an email notification to the ICANN org when a Contracted Party submits a request for an exemption of automated processing of a specific category of disclosure requests.

A1.11.16. Internet User to ICANN org

A1.11.16.1. Process to View Quarterly SSAD Status Reports/Dashboard

Related Recommendation(s): #17

Internet users may access public reporting on the use and functioning of the SSAD through the ICANN org portal. Reports will be published on a quarterly basis including summary details of at least:

- Number of disclosure requests received.
- Average response times to the disclosure requests, categorized by priority level.
- Number of requests categorized by third-party purposes/justifications.
- Number of disclosure requests approved and denied.
- Number of disclosure requests automated.
- Number of requests processed manually.
- Information about financial sustainability of SSAD.
- New EDPB guidance or new topical jurisprudence (if any).
- Technical or system difficulties.
- Operational and system enhancements.

A1.11.16.2. Submit Report of Abusive Behavior

Related Recommendation(s): N/A

The ICANN org will allow public Internet users to report abusive behavior in the SSAD through the ICANN org portal.

A1.11.17. Auditors to AA, Accredited Requestors

A1.11.17.1 Audit process

Related Recommendation(s): #1.4.8, #2.4, #16

Audits to ensure appropriate monitoring and compliance with the process requirements and SSAD terms of use will be performed by the auditing firm(s) according to the auditor evaluation model for the corresponding entity of the SSAD including the Central and Governmental Accreditation Authorities, and Accredited Requestors. In the case of Accreditation Authorities,

an initial audit must be conducted prior to becoming fully operational. During the rest of the first and second year, the auditors would monitor and follow up on any discrepancies or outstanding issues. Subsequent audits will focus on collecting evidence based on a risk and materiality analysis, including reports of any internal audit conducted by the Accreditation Authority and also collecting samples within areas of importance for the community, to ensure the internal audit works as intended.

Governmental AAs will have the option to either be audited by the Central Accreditation Authority Auditor, or provide to the ICANN org the audit report of an audit conducted by an auditor chosen and paid by the Governmental AA. Audits of a Governmental AA will be against their accreditation policy.

For Governmental AAs and Accredited Requestors, audits are expected to be based on a sample of requests, to ensure they are legitimate and do not violate policy. This can be done through the CG's audit trail.

A1.11.18. AA Auditor to ICANN org

A1.11.18.1. Report Accreditation Authority Audit Results

Related Recommendation(s): #1.4.8, #2.4, #16

Audit evaluation results of the Accreditation Authority are to be provided to ICANN org to determine if any action or remediation is required from the Accreditation Authority.

A1.11.19. Accredited Requestor Auditor to Central AA

A1.11.19.1 Reporting Process Accredited Requestor Audit Results

Related Recommendation(s): #1.5.4, #16.2, #16.10

Audit evaluation results of the Accredited Requestors are to be provided to the Central Accreditation Authority to determine if any action on the Requestor is required.

A1.12. System Logging in SSAD

Per Recommendation 15, and in accordance with the data retention policy of the SSAD, logging procedures are expected to be in place by the sub-service providers in SSAD:

- Central and Governmental Accreditation Authorities.
- Central Gateway Manager.
- Identity Provider (if applicable).
- Contracted Parties.

Sub-service providers in the SSAD are expected to log the details of all transactions to facilitate the auditing procedures, including the activity of accredited users such as login attempts, queries, disclosure decisions made, and disclosure of nonpublic data.

At a minimum, the following events will be logged:

- Logging related to the identity provider.

- Logging related to the Accreditation Authority.
    - Details of incoming requests for accreditation.
    - Results of processing requests for accreditation, e.g., issuance of the Identity Credential or reasons for denial.
    - Details of revocation requests.
    - Indication when identity credentials and declarations have been validated.
    - Unique reference number.
- Logging related to the Central Gateway Manager
    - Information related to the contents of the query itself.
    - Results of processing the query, including changes of state (e.g., received, pending, in-process, denied, approved, approved with changes).
    - Rates of:
        - Disclosure and non-disclosure.
        - Use of each reason for denial for non-disclosure.
        - Divergence between the disclosure and non-disclosure decisions of a Contracted Party and the recommendations of the CG.
- Logging related to Contracted Parties:
    - Request response details (e.g., reason for denial, notice of approval and data fields released). Disclosure decisions including a reason for denial must be stored.

A1.13. Data Retention Policy

The data retention policy for the SSAD will require all SSAD sub-service providers to preserve all operational data and system logs for a total of 18 months.

The 18-month time period for data retention is derived from the audit cycle, currently considered to be of one year, plus six months for audit review and processing.

A1.14. System Support

For the Central AA and the CG system components, the following service level agreement (SLA) is being considered:

- 24x7 customer support.
- 99.9% system availability (8.77 hours of downtime per year).
- Response times under four seconds for 95% of requests.

A1.15. References

Below are links to resources used in preparation of this appendix. These can also be found as footnotes to specific references.

1. Final report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process. https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf
2. TSG01: Technical Model for Access to Nonpublic Registration Data. https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf
3. Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect. https://datatracker.ietf.org/doc/draft-ietf-regext-rdap-openid/

4. RFC 8982: Registration Data Access Protocol (RDAP) Partial Response. https://datatracker.ietf.org/doc/html/rfc8982
5. OpenID Connect Core. https://openid.net/specs/openid-connect-core-1_0.html
6. OAuth Assertion Framework. https://datatracker.ietf.org/doc/html/rfc7521

Appendix 2 — Global Public Interest Considerations

A2.1. Background

In late 2019, the ICANN Board developed a proposed global public interest (GPI) framework in consultation with the ICANN community. The framework is designed to demonstrate whether and how specific advice and recommendations developed by the community serve the global public interest within ICANN's remit.

At the conclusion of the community consultation on the proposed framework, the Board agreed to pilot the proposed GPI framework and showcase how it can be leveraged to ascertain relevant public interest considerations on a given issue, identify gaps, if any, and share lessons learned.

Following its commitment, the Board identified the System for Standardized Access/Disclosure (SSAD) as the first test case for the pilot. Specifically, the Board oversaw ICANN org's running of the pilot to look at the GPI considerations of the SSAD policy recommendations, as proposed in the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process from the Generic Names Supporting Organization (GNSO).

This document provides an overview of the process and findings of the pilot conducted by ICANN org and outlines next steps.

A2.2. Pilot Scope

The scope of the SSAD GPI pilot consists of the following activities:

1. Pilot the draft framework to demonstrate a post-facto assessment of how the community appeared to address and consider various public interest considerations as they crafted the recommendations.

2. Assess the extent to which all of those considerations could have been further facilitated by using the GPI framework.

3. Identify how the use of the GPI framework could be leveraged in future community work to ascertain the GPI in a more consistent and predictable manner.

A2.3. Summary of Process

ICANN org developed a four-step process, outlined below, to explore which recommendations carry public interest considerations, how the community-developed recommendations fit within the framework, and lastly, how the framework could have been leveraged to facilitate and standardize the GPI approach across the ICANN community.

Step 1: Review relevant documentation to determine which recommendations may carry public interest considerations.

Step 2: Determine and map which of the five overall GPI framework categories are relevant to each of the identified recommendations from Step 1.

Step 3: Apply the questions posed in the framework to consider the GPI issues in light of the relevant ICANN Bylaws.

Step 4: Weigh the various considerations and viewpoints, including minority statements, resulting in a balanced recommendation that takes into account all of the relevant inputs.

A2.4. ICANN org Application of the Framework

The process described in A.2.3. was applied to demonstrate one possible example of the application of the framework. ICANN org reviewed the EPDP Phase 2 Team's Final Report, output from public comment forums held throughout the policy development process, and other relevant materials, for evidence to support the community's public interest considerations, without supplanting ICANN org's own evaluations.

Of the twenty-two recommendations evaluated under the pilot, there were eight individual recommendations identified as possible candidates that may carry public interest considerations. These same eight recommendations also resulted in "strong support but significant opposition" or "divergence" designations from the community.

The eight identified recommendations were 5, 6, 8, 9, 10, 12, 14 and 18 and they fall into three of the five overall framework categories: Stability and Security [ICANN's technical coordination]; Accountability and Transparency [ICANN's policies and practices]; and Fiscal Responsibility [ICANN's policies and practices].

Below is the output of the exercise to apply the framework to the SSAD recommendations, capturing one possible use of the framework. The information is organized by the relevant GPI framework categories, as well as the rationale and additional viewpoints considered by the community.

1. **Stability and Security** | *Relevant Recommendations* - 6, 8, 10

Bylaws Considerations Considered by the Community

- Will it "preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet"? (Commitment a.i)

Rationale Considered by the Community

- The community has demonstrated a commitment to the GPI by contributing to the security and stability of the Internet; access to gTLD registration data supports GPI efforts relating to consumer protection, cybercrime investigation, prosecution of DNS abuse and intellectual property infringement, law enforcement needs, and the identification and correction of network administration problems to maintain Internet stability.

Additional Viewpoints Considered by the Community

- Some community groups raised concerns that the recommendations could adversely impact the security and stability of the DNS, as well as public health and safety (i.e., critical infrastructure and child exploitation), physical and economic security, and

national security.

- The current classification of cyber security threats (including threats to consumer protection and those that affect public concerns and the overall security of the DNS) as "Priority 3," has been flagged by a few community groups, who note that it may be insufficient to address the reality of serious online threats, as well as too slow to deliver data at speeds to satisfy operational security needs.

2. **Accountability and Transparency** | *Relevant Recommendations* - 5, 8, 9, 12, 18

Bylaws Considerations Considered by the Community

- Will it "make decisions by applying documented policies consistently, neutrally, objectively, and fairly, without singling out any particular party for discriminatory treatment (i.e., making an unjustified prejudicial distinction between or among different parties)"? (Commitment a.v)

- Will it "remain accountable to the Internet community through mechanisms defined in these Bylaws that enhance ICANN's effectiveness"? (Commitment a.vi)

- Will it "operat[e] with efficiency and excellence, in a fiscally responsible and accountable manner and, where practicable and not inconsistent with ICANN's other obligations under these Bylaws, at a speed that is responsive to the needs of the global Internet community"? (Core value b.v)

Rationale Considered by the Community

- Transparency and accountability are at the core of SSAD; its stated objective is to "provide a predictable, transparent, efficient, and accountable mechanism for the access/disclosure of nonpublic registration data," and the language of transparency appears in multiple recommendations.

- ICANN has a commitment to ensuring documented policies are followed consistently, neutrally, objectively, and fairly; the automation proposed with respect to request intake and routing in SSAD can help to ensure neutrality and objectivity.

Additional Viewpoints Considered by the Community

- Some concerns were raised that the technical aspects of automation could bear review with regard to reliability, accuracy, and transparency, and that there are potential safety and security implications with regard to revealing the identities of data Requestors, which may compromise investigations and endanger the safety and rights of data Requestors.

- Public interest concerns of accountability, objectivity, and security overlap when considering the evolution mechanism and decentralization. Another consideration was that the decentralized system could potentially result in higher costs, slower request processing, security risks, and the possibility for subjective judgment. A consistent, scalable system could potentially enhance objectivity, as well as the trust and accountability of the DNS more generally.

3. **Fiscal Responsibility** | *Relevant Recommendation* - 14

Bylaws Considerations Considered by the Community

- Will it "operat[e] with efficiency and excellence, in a fiscally responsible and accountable manner and, where practicable and not inconsistent with ICANN's other obligations under these Bylaws, at a speed that is responsive to the needs of the global Internet community"? (Core value b.v.)

Rationale Considered by the Community

The community has considered financial sustainability in Recommendation 14, which defines an objective of having the SSAD be financially self-sufficient without causing any additional fees for registrants. While this recommendation notes that requestors of the SSAD data should primarily bear the costs of maintaining this system, it also states that ICANN "MAY contribute to the (partial) covering of costs for maintaining the Central Gateway."

Additional Viewpoints Considered by the Community

- While this proposed financial structure may have clear benefits for ICANN's financial sustainability, community groups raised concerns that these benefits may come at the expense of security and stability, as the costs incurred by Requestors may deter use. Since Requestors are currently expected to pay most costs for the SSAD, costs for Requestors, including those combating security threats, may be significant.

- Some community groups propose alternative financial structuring, including ICANN-subsidized funding, as well as a cost-benefit analysis which could help to uphold ICANN's security and stability mandate; ensure a commitment to fiscal responsibility, not only for ICANN itself, but also those using its services; and contribute towards being responsive to the needs of the global Internet community.

A2.5. Observations

Throughout the pilot, several observations were made regarding the framework.

- The ICANN community considered and addressed public interest considerations in the rationales provided in the SSAD recommendations. This was particularly evident across three broader themes/categories identified during the pilot as having public interest implications and considerations.

- Though the ICANN community did not formally use the GPI framework, the community took the GPI into account through its bottom-up, multistakeholder policy development processes.

- While there remain areas of divergence on these recommendations' topics, those have been documented and addressed through the bottom-up, multistakeholder policy development process, as called for in the ICANN Bylaws.

- The pilot process demonstrates that the GPI exercise will be far more effective when the framework is initially run as part of recommendation development, as opposed to a post-facto review.

- The GPI is a key consideration in ICANN's work and evaluation of the GPI under this framework, or any other tool or process, could be considered for use at any time during the lifecycle of recommendations.

- While the application of the GPI framework shows that the recommendations appear to be in the public interest, the ICANN Board will have additional considerations before deciding if the recommendations are within the best interests of ICANN and the ICANN community, which could call other measures of the public interest into question. For example, potential costs in implementation of the recommendations may rise to a high enough level that the ICANN Board might have to consider how those costs impact ICANN's ability to continue to serve its mission and the public interest more broadly.

A2.6. Conclusion and Next Steps

This document illustrates how the community takes the GPI into account through its processes and demonstrates how the community could potentially apply the specific categories of the GPI framework and the framing Bylaws questions in its decision-making process.

The community is strongly encouraged to consider the use of the framework in its future work as a way to help structure and guide its discussions on the GPI. The considerations and questions outlined in the framework could help make the process of ascertaining the GPI more consistent and predictable, while also formally documenting and creating a record of those considerations and questions for consistency.

In turn, this will help clearly communicate to the Board how GPI considerations were taken into account by the community and inform the Board's subsequent discussions and actions. In addition, it will help to reinforce the commitment to the public interest and to keep the conversations around the GPI active in the community dialogue.

Finally, the Board has identified the New gTLD Subsequent Procedures policy recommendations, in the context of the ODP, as the second test case for the pilot of the GPI framework.

Appendix 3 — Operational Design Assessment Data Collection Methodology

ICANN org conducted various data collection efforts upon which to base and build the analysis captured in this Operational Design Assessment.

A3.1. Community Engagement

The ODP is meant to address a number of issues as noted in the Operational Design Phase - Process paper. Among those issues, transparency is of significant importance and focus. Since the start of the SSAD ODP, ICANN org provided updates to the community on the status of the overall effort, provided specific design updates and requested feedback. ICANN org has conducted five community webinars, two GAC specific webinars, one GNSO Council specific webinar, and held monthly meetings with the GNSO Council Liaison. These are collectively captured in the SSAD ODP specific webpage, www.icann.org/ssadodp. As outlined in the aforementioned process paper, these engagements were held to receive feedback on:

1) Facts, figures, and assumptions that ICANN org used for its ODP assessment.
2) Ensuring there are no inconsistencies in ICANN org's assessment of the recommendations with existing Consensus Policies or other relevant work.
3) Considerations, relevant to the scope set by the Board, from stakeholders who are expected to execute recommendations or are otherwise affected by them.
4) Requests from ICANN org or the Board for specific inputs from the community.

Through the GNSO Council Liaison, ICANN org received clarifications or confirmations on a total of 12 topics. All email exchanges with the GNSO Council Liaison as well as community feedback were published in the publicly archived mailing list.

A3.2 Request for Information (RFI)

To supplement ICANN org knowledge regarding solutions available in the marketplace, ICANN org opened a public RFI from 21 June 2021 to 19 July 2021. The RFI included questions regarding:

- Identity verification services and methods.
- Additional services to conduct verification of various characteristics of legal and natural persons including affiliation with organizations.
- System development methods, effort, and ranges of costs.

For all services, the RFI requested details about jurisdictional availability and cost estimates. Furthermore, the RFI offered any respondent the opportunity to provide any other information they wanted to share with ICANN org related to the SSAD.

Seventeen organizations provided full or partial responses to the RFI. All responses were reviewed with the applicable team members and informed the topic areas within the ODA. Responses are described generally and there is no identification of specific respondents to maintain confidentiality.

A3.2.1. RFI Response Analysis

Lack of Pricing Information

Many RFI respondents did not offer pricing information because their services are available along a risk and price continuum, often called assurance level.

Limitations of Responses Received
RFI responses were limited to specific elements of the RFI and did not typically consider how such responses might be incorporated into a more complex set of systems and processes. Responses that contemplated a complete system to solve for all SSAD needs were likewise vague as many details are still unknown or are meant to be addressed during implementation.

Of the handful of responses that provided identity verification process information, all were largely limited to that for Natural Persons.

There were very few responses that identified existing capabilities for verifying requestor declarations. ICANN org kept the RFI's structure and content as general as possible to encourage a wide variety of submissions. For those respondents with solutions that vary based on the acceptable level of risk, they did not provide exact solutions, costs, and availability.

Challenges of Representation or Affiliation Verification
The GNSO-approved recommendations do not provide details on acceptable levels of verifications for Requestor Declarations, nor are specific standards provided. One example could be the verification of a power of attorney. Without a particular standard, it is unclear what constitutes "verification." Methods might include:

- Checking for the existence of the associated law firm.
- Checking if the lawyer existed as a recognized practitioner at the time the document was executed.
- Checking if the lawyer was ever affiliated with the named firm.
- Checking with the individual who requested to grant power of attorney to another person.

This example exposes several related questions/issues:

- If the law firm no longer exists it does not necessarily invalidate the document.
- Similarly, the lawyer may not be able to be verified as a practicing attorney at a given point in time in the past.
- If any party, legal or natural, needs to be contacted to verify the validity of the document, do any or all of them need to be formally identified, similar to a SSAD-accredited user?

A3.2.2. Request for Information Questions

ICANN org asked the following questions of potential vendors to gather data about their organizations, pricing, products, and services.

General Questions About the Organization

- Legal name of firm/entity.
- Name of the contact person for this RFI.
- Role/designation of the contact person for this RFI.
- Email address of the contact person for this RFI.
- Contact information (address, contact number, etc.) of the contact person for this RFI.

Questions About Identity Verification Services

- Describe, in general terms, your methodology(ies) for verifying the identity of a Legal Person. Please include a description of any anti-impersonation measures you have in place.

- Describe, in general terms, your methodology for verifying the identity of a Natural Person. Please include a description of any anti-impersonation measures you have in place.
- Describe, in general terms, your methodology for renewing or extending identity verification for a Legal Person.
- Describe, in general terms, your methodology for renewing or extending identity verification for a Natural Person.
- For each service you offer, which jurisdictions are supported?
- Are there any regions, territories, countries, or jurisdictions in which you are unable to identify either Legal or Natural Persons? If so, why?
- How are your methods unique in the marketplace?
- Do you have established methods for individuals to undergo additional review or evaluations if your primary methods are insufficient?
- After a Legal or Natural Person has been verified, how long do you consider that identification valid?
- Do you monitor any verified data sources for changes that might trigger a need for re-verification? (e.g., death of an individual, dissolution of a legal entity, etc.?)
- After verification has completed, do you have any methods or services that ensure that the identified individual is the same individual when the identity credential or equivalent is later used? (i.e., is the identified person the same person using the verified identity?)
- For all methodologies you are describing, how is the need to comply with applicable data protection laws taken into account?

Questions About Additional Verification Services

- Describe any services you offer to verify characteristics of legal or natural persons. Such characteristics might include occupation, employer, professional affiliation, ultimate beneficial owner, affiliates, membership in a particular industry, participation in a major stock exchange, status as a government employee or entity, status as an IGO/NGO, etc.
- For each of the areas you have identified in your response to the previous question, provide a range of fees for such services and for which jurisdictions each is available. When providing an answer to this question, please use the template attached.
- Describe any services you offer to verify compliance of an identified person with applicable data protection laws and/or practices. For each, provide a range of fees for such services and for which jurisdictions each is available. When providing an answer to this question, please use the template attached.
- Describe any services you offer to verify the validation of a power of attorney (or local equivalent). For each, provide a range of fees for such services and for which jurisdictions each is available. When providing an answer to this question, please use the template attached.
- Describe any other verification services you offer that may be relevant and associated fees and availability by country or jurisdiction. When providing an answer to this question, please use the template attached.
- Describe the customer service and support functions you offer and associated fees and availability by country or jurisdiction. When providing an answer to this questions, please use the template attached.
- Describe any services you offer for supporting challenges to a failed identification attempt and a range of fees and availability by country or jurisdiction (if applicable). When providing an answer to this question, please use the template attached.

Questions About Level of Effort Needed for System Design

- Provide an estimate of effort it would take (in hours), within a +/- 20% range, for the system design of the Central Gateway?
- Provide an estimate of effort it would take (in hours), within a +/- 20% range, for the system development of the Central Gateway?
- Provide an estimate of effort it would take (in hours), within a +/- 20% range, for the on-going maintenance of the developed system?
- Provide an estimate of effort it would take (in hours), within a +/- 20% range, for the on-going operations of the central gateway?
- Provide an estimate of the average hourly rate for the above-mentioned efforts.
- Provide an estimate of the amount (dollars), within a +/-20% range, for any additional fees that may be needed for anything not covered elsewhere.

Any Additional Information

- If you have any additional information, ideas, knowledge, assumptions, or comments related to this initiative that you think would be beneficial to share, please provide a file attachment of the same here.

A3.3. Contracted Parties Questionnaire

In order to inform the team's analysis of feasibility and associated risks, costs and resources required in the potential implementation of the SSAD, ICANN org conducted a Contracted Parties questionnaire which related to the following Board scoping questions:

> 3.1.5.2: What is the expected volume the SSAD operational process flow will be able to manage?
> 3.1.5.5: How many potential users may be expected to use the system?

The Contracted Parties questionnaire focused on the total number of disclosure requests received for nonpublic registration data. These responses provided one input to help estimate the potential volume of requests that SSAD would support.

The Contracted Parties questionnaire was available online and included a combination of open responses, multiple choice, and Likert scale questions. The Contracted Parties questionnaire opened on 5 July 2021 and initially was scheduled to close on 19 July 2021. ICANN org staff conducted the outreach through various avenues to promote the Contracted Parties questionnaire. In order to obtain additional feedback, the Contracted Parties questionnaire remained open for an additional month, closing on 20 August 2021.

A3.3.1. Questions Asked of Contracted Parties

1. Approximately, how many domain names does your organization manage? (Please provide a single aggregate if you operate multiple gTLDs or multiple ICANN registrar accreditations.)
2. During 2019, what was the monthly average number of requests to disclose nonpublic domain name registration data for domains in gTLDs that your organization received?
3. During 2020, what was the monthly average number of requests to disclose nonpublic domain name registration data for domains in gTLDs that your organization received?
4. How many total (all time) unique Requestors have sent disclosure requests to your organization for access to nonpublic domain name registration data for domains in gTLDs?

5. What additional categories of users, besides the ones listed below, have submitted requests for access to nonpublic) domain name registration data for domains in gTLDs to your organization?
    a. Law Enforcement
    b. Cyber security professional
    c. Intellectual property holder/brand protection entity
    d. Legal professional
    e. Certificate authorities
6. Please indicate whether other members of your organization are likely to participate.

A3.3.2. Contracted Parties Questionnaire Response Analysis

- There were a total of 86 responses received.
- 35% of the participants identified as Registry Operators and 65% identified as Registrars.
- Total number of Domains Under Management (DUM) reported was roughly 167 million.
- 65 million is the highest reported number of domain names managed.
- Registrars reported they received a maximum of 699 requests a month.
- Registries reported they received a maximum of 1000 requests a month.

The full analysis summary for the Contracted Party questionnaire can be found in Appendix 4.

A3.4. Community Questionnaire

In order to inform the team's analysis of feasibility and associated risks, costs and resources required to in the potential implementation of the SSAD, ICANN org also conducted a questionnaire for the general ICANN community which relate to the same Board Scoping questions as above.

> 3.1.5.2: What is the expected volume the SSAD operational process flow will be able to manage?
> 3.1.5.5: How many potential users may be expected to use the system?

The community questionnaire focused on the estimated number of disclosure requests sent to Contracted Parties and gauging the potential interest among stakeholder groups in using the SSAD.

The community questionnaire was available online and included a combination of open responses, multiple choice, and Likert scale questions. The community questionnaire opened on 5 July 2021 and initially was scheduled to close on 19 July 2021. ICANN org conducted the outreach through various avenues to promote the community questionnaire. In order to obtain additional feedback from the community, the community questionnaire remained open for a little over a month, closing on 6 August 2021.

A3.4.1. Community Questionnaire Questions

1. In what jurisdiction (country/territory) do you or your organization primarily function?

2. During 2019, what was the monthly average number of requests to disclose nonpublic generic top-level domain (gTLD) domain name registration data that your organization submitted?
3. During 2020, what was the monthly average number of requests to disclose nonpublic generic top-level domain (gTLD) domain name registration data that your organization submitted?
4. If implemented, how likely are you or your organization to use the System for Standardized Access/Disclosure (SSAD) to request nonpublic registration data?
5. If the System for Standardized Access/Disclosure (SSAD) is implemented, what do you estimate would be the monthly average number of requests to disclose nonpublic generic top-level domain (gTLD) domain name registration data that you or your organization would submit?
6. What additional categories of users, besides the ones listed below, do you or your organization believe would be interested in using the System for Standardized Access/Disclosure (SSAD) to access nonpublic domain name registration data?
    a. Law Enforcement
    b. Cyber security professional
    c. Intellectual property holder/brand protection entity
    d. Legal professional
    e. Certificate authorities
7. What factor(s) would be most important to you in determining whether to use the System for Standardized Access/Disclosure (SSAD)?

A3.4.2. Community Questionnaire Response Analysis

- There were a total of 355 responses received.
- The largest number of participants (42%) identified themselves as government agencies.
- The majority of responses came from the United States, Canada, and Europe.
- 78% of participants noted that they would use the SSAD if implemented to request nonpublic registration data.
- Some groups such as academic researchers and government agencies seemed to indicate higher demand for the SSAD.
- Some countries/jurisdictions such as Europe, and the United States seem to predict a higher demand for the SSAD.

The full analysis summary for the community questionnaire can be found in **Appendix 5.**

A3.5. GAC Outreach Questionnaire

ICANN org sent an outreach questionnaire to the Governmental Advisory Committee, asking three questions for respondents and nine optional questions intended to collect further input relevant to the implementation of Recommendation #2 and the way a government/territory would engage with the SSAD.

The GAC questionnaire was available online. The GAC questionnaire opened on 15 July 2021 and initially was scheduled to close on 17 September 2021. In order to obtain additional feedback from the GAC, the GAC questionnaire remained open for over three months, closing on 31 October 2021.

The survey yielded 16 responses, with three duplicates, hence a total of 13 unique responses. Out of the 13 unique responses:

- Three countries/territories only provided their names
- Ten countries/territories provided answers to all three basic questions
  - Seven of them also responded to all optional questions
  - Two of them responded to part of the optional questions
  - One responded to none of the optional questions

With respect to the basic questions, the countries/territories that responded suggested different governmental bodies depending on the allocation of competencies within each administration, as the responsible body to select or set up a Governmental AA. Some suggested the same bodies designate to ICANN org or its designee the selected Governmental AA. Some suggested the selected Governmental AA is designated to ICANN org or its designee through the representatives in the GAC.

A3.5.1. GAC Survey Questions

The GAC Outreach Questionnaire included three primary questions and an additional nine optional questions. These are presented below as they were in the survey.

1. Which country/territory are you representing?
2. How should each country/territory or Government-designated Accreditation Authority (AA) be designated to ICANN org or its designee?
3. Who in your administration should be authorized to make such designations?

The following questions are meant to collect further input relevant to the implementation of recommendation #2 and the way your government/territory would engage with the SSAD. Please consider them optional.

4. How would the SSAD AA for your jurisdiction accredit governmental entities (and legitimate users within these entities)?
5. Is there an entity that performs a comparable verification process in your jurisdiction today? Provided you intend to implement recommendation #2 for accrediting your eligible government entities, could that authority take on the role of the AA for the purposes of the SSAD?
6. If not, which authority could take on the role of the AA for the purposes of the SSAD?
7. Could the role of the SSAD AA for your jurisdiction or for specific categories of governmental entities in your jurisdiction (e.g. law enforcement agencies) be delegated to an IGO that could perform the role of the SSAD AA in multiple jurisdictions?
8. Under what legal basis(es) may authorities in your jurisdiction request disclosure of nonpublic registration data by registries/registrars?
9. Under what legal basis(es) may authorities in your jurisdiction request disclosure of nonpublic registration data by registries/registrars in another jurisdiction?
10. Under what legal basis(es) may authorities in another jurisdiction request disclosure of nonpublic registration data by registries/registrars in your jurisdiction?
11. Are there legal requirements for transfer of registration data that contain personal data outside your jurisdiction? If yes, what are those?
12. Please provide any further input you see relevant to the accreditation of governmental entities and requests for disclosure of nonpublic registration data by governmental entities.

A3.6 Market Research

To supplement the community and contracted party surveys to collect additional data from outside the ICANN world, ICANN org sought to engage with a market researcher, who can professionally survey the various professions globally. The research is aimed to gain more data around the expected volume of the requests, the number of SSAD users, and their price sensitivity. This information will aid in the development of the system and supporting processes. Overall, such information contributes to the estimate for system cost which is a major component of determining user fees and financial self-sustainability.

The Board's questions outlined in the Scoping Document cover various aspects of demand, usage and financial models:

- **3.1.5.2.** What is the expected volume the SSAD operational process flow will be able to manage?
- **3.1.5.3.** Can the SSAD handle requests for nonpublic registration data in a timely and predictable manner?
- **3.1.5.4.** Can the SSAD design scale to meet reasonably anticipated, future operational changes, for example as anticipated in Recommendation 18?
- **3.1.5.5.** How many potential users may be expected to use the system?
- **3.2.1.** What systems, tools, and infrastructure are needed for the technical operation of the SSAD and its component parts?
- **3.5.2.** How will the fee structure for the SSAD be constructed?

The ODP Project team contacted 11 reputable firms to solicit proposals for this work. Due to the scope of the work, some firms turned down the work, others submitted proposals that would not adequately answer the questions posed. With the difficulty finding the appropriate market researcher, ICANN org made a decision to conduct this research work outside the ODP project. When the org identifies the appropriate firm to conduct this work, the research will be conducted and the analysis will be submitted to the Board separately from the ODP.

Appendix 4 — Contracted Parties Questionnaire Analysis Summary

- A total of 86 responses were received for the Contracted Party questionnaire.
- 35% of the participants identified as registry operators and 65% identified as registrars.

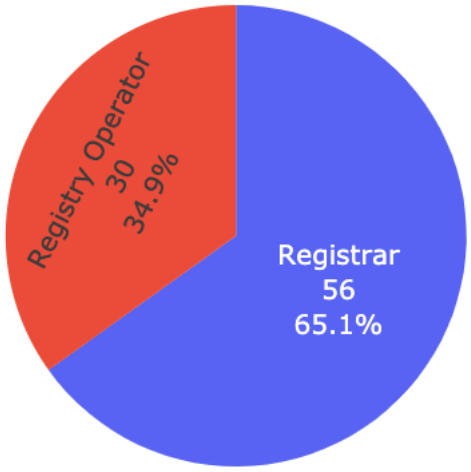

Figure A4-1. Contracted Party questionnaire respondents by type.

- Overall, the total number of domains under management (DUM) reported was roughly 167 million.
- The results displayed a varying number of domain names managed by participants. The highest number of domain names managed by a single registrar was 65 million and 10.5 million by a single registry. As it was optional to participate in this questionnaire it is important to note that these results do not provide a full representation of the number of domains managed per registrar and registry operator.

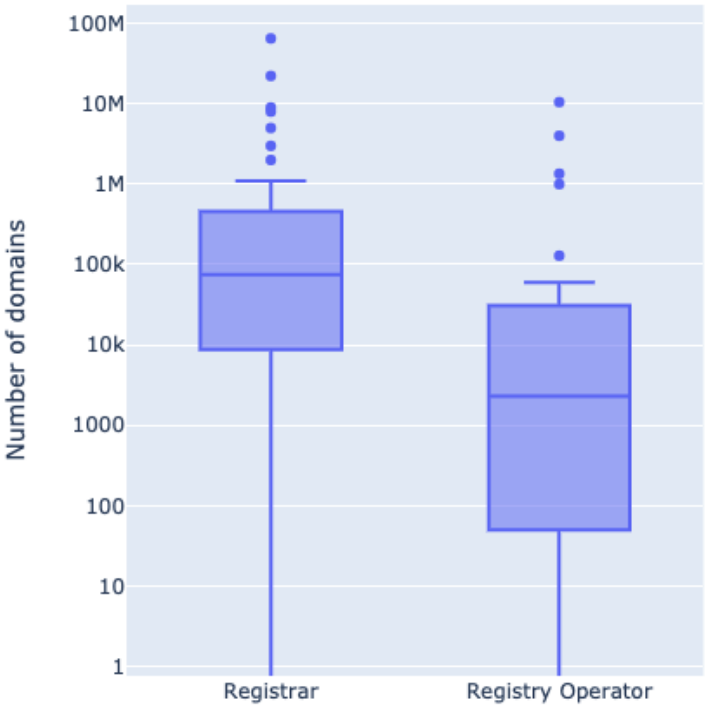

Figure A4-2. Number of domains under management by type of contracted party respondent.

- In total, registrar respondents reported a maximum of 699 requests a month to access nonpublic registration data. Registry operator respondents reported a maximum of 1000 requests a month to access nonpublic registration data.
- Overall, most respondents (58 participants) noted receiving less than 10 requests a month to access nonpublic registration data in 2019 and 2020.
- Furthermore, in 2019, 16 participants noted receiving between 10 to 50 requests a month and four participants noted receiving 50 to 149 requests a month to access nonpublic registration data. In 2020, 11 participants noted receiving 10 to 50 requests per month and seven participants noted receiving 40 to 149 requests a month to access nonpublic registration data.

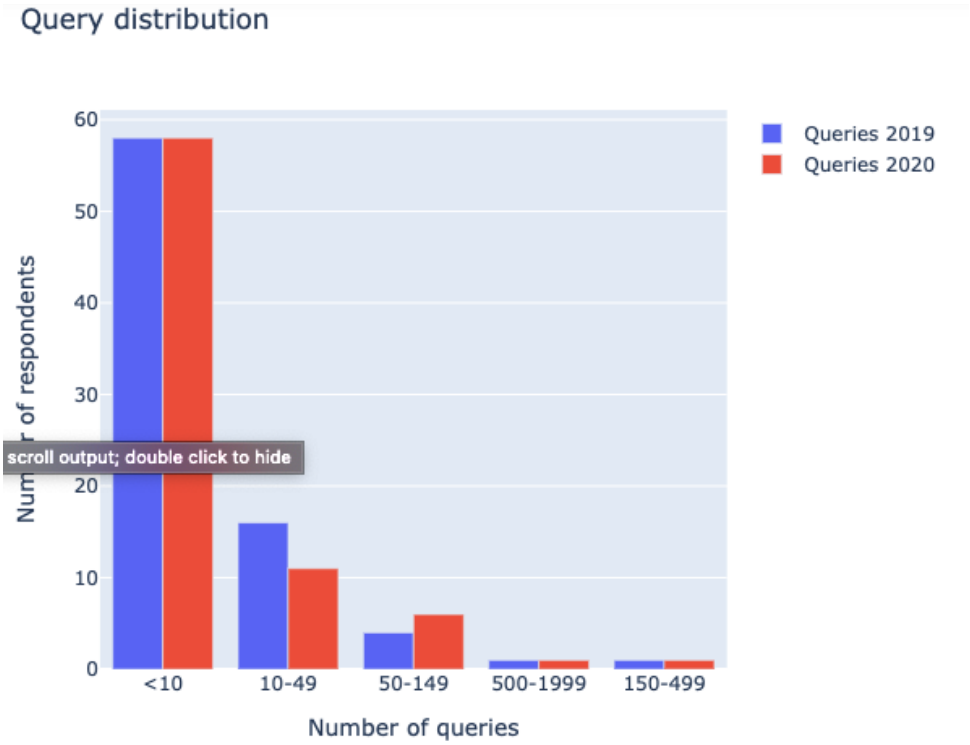

Figure A4-3. Number of Contracted Parties' reported data disclosure requests per month.

- Both registrars and registries identified the general public as an additional group who would be interested in using the SSAD to access nonpublic registration data.

Appendix 5 — Community Questionnaire Analysis Summary

- A total of 355 community members participated in the questionnaire.
- The largest number of participants (42%) identified themselves as government agencies. The second and third largest group of participants were legal and business professionals, with 17% and 14% respectively. This distribution may be representative of how often groups may use the SSAD if implemented.
- Other participant groups included intellectual property holder/brand protection entities (13%), cyber security professionals (8%), ISP or web hosting providers (4%), academic researchers (1%) and certificate authorities (0.84%)
- As shown in **Figure A5-1**, most responses came from the United States, Canada, and Europe (Germany, United Kingdom, Switzerland, Italy, Spain, France). A small number of responses came from the Asia Pacific, Latin America and the Caribbean, and Africa regions. This may indicate a non-response bias and generally represents the dynamics of the active participants within the ICANN community. It is important to keep this in mind as it may not fully represent potential SSAD users. This may also indicate that the lack of participation from non-Western countries is due to the sentiment that data protection laws such as GDPR do not necessarily apply to them.

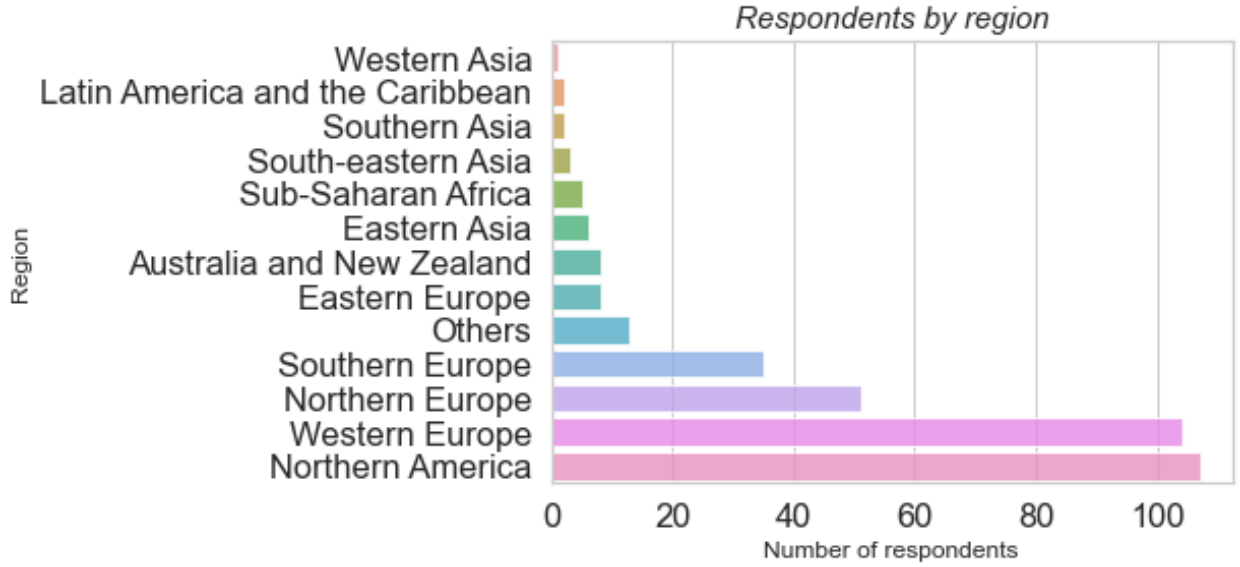

Figure A5-1. Community survey respondents by region.

- 78% or 252 participants noted that they would use the SSAD, if implemented, to request nonpublic registration data. See **Figure A5-2**.

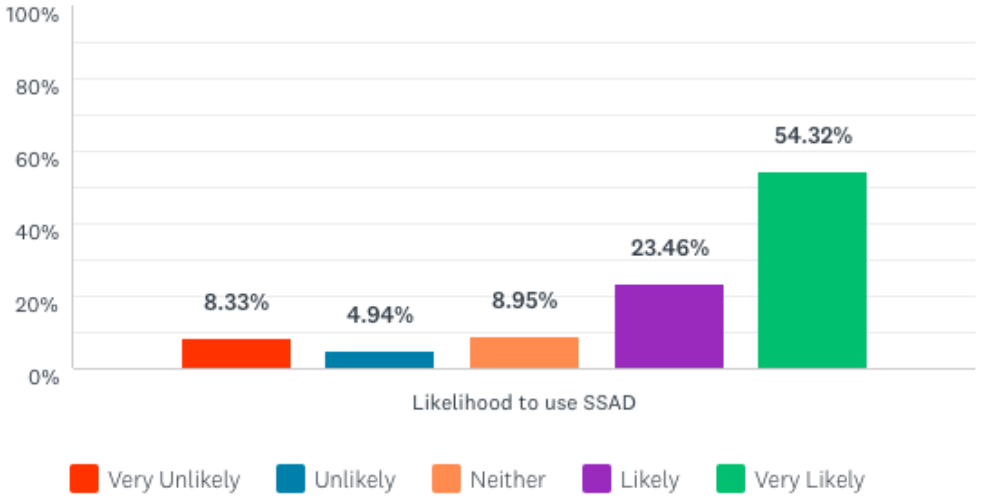

Figure A5-2. Community respondents' reported likelihood of using SSAD.

- In 2019, roughly 180 respondents sent less than ten queries per month, 20 respondents sent 50 to 500 queries per month, and 10 respondents sent over 2,000 queries per month to access nonpublic registration data.
- In 2020, roughly 130 respondents sent less than ten queries per month, 30 respondents sent 50 to 499 queries per month, and 30 respondents sent over 2,000 queries per month to access nonpublic registration data.
- If the SSAD is implemented, respondents predicted a slightly higher number of queries would be sent to access nonpublic registration compared to the previous years above.

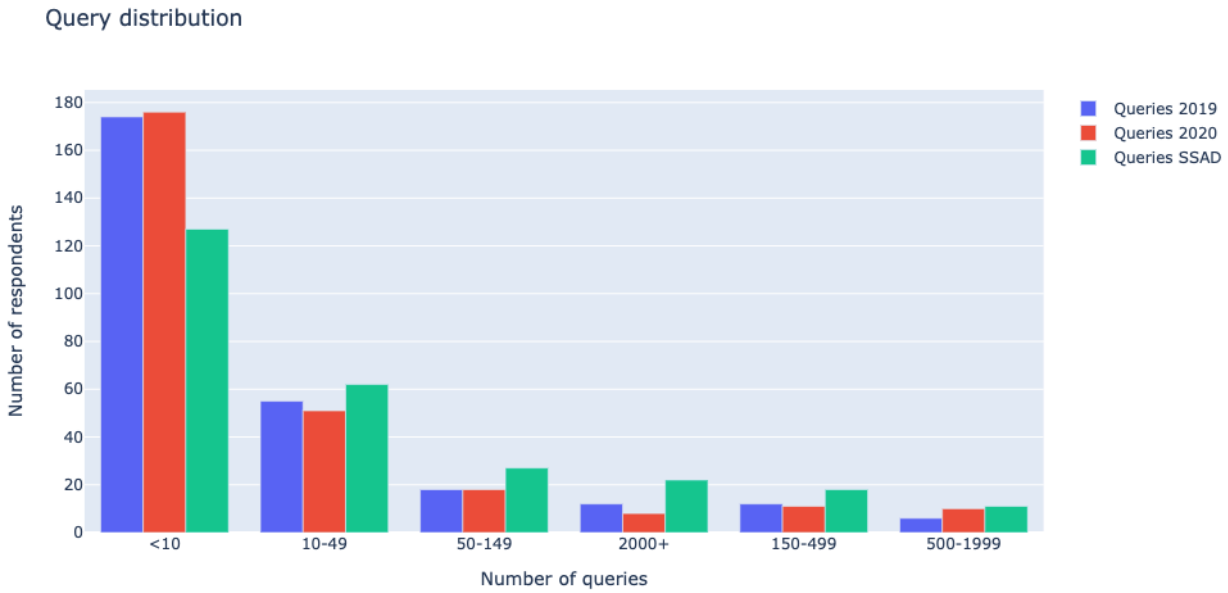

Figure A5-3. Reported and projected number of queries per month.

- Some groups, such as academic researchers, government agencies, legal professionals, and cyber security professionals, seemed to have a higher demand for the SSAD, where they anticipate sending up to 100,000 queries per month.

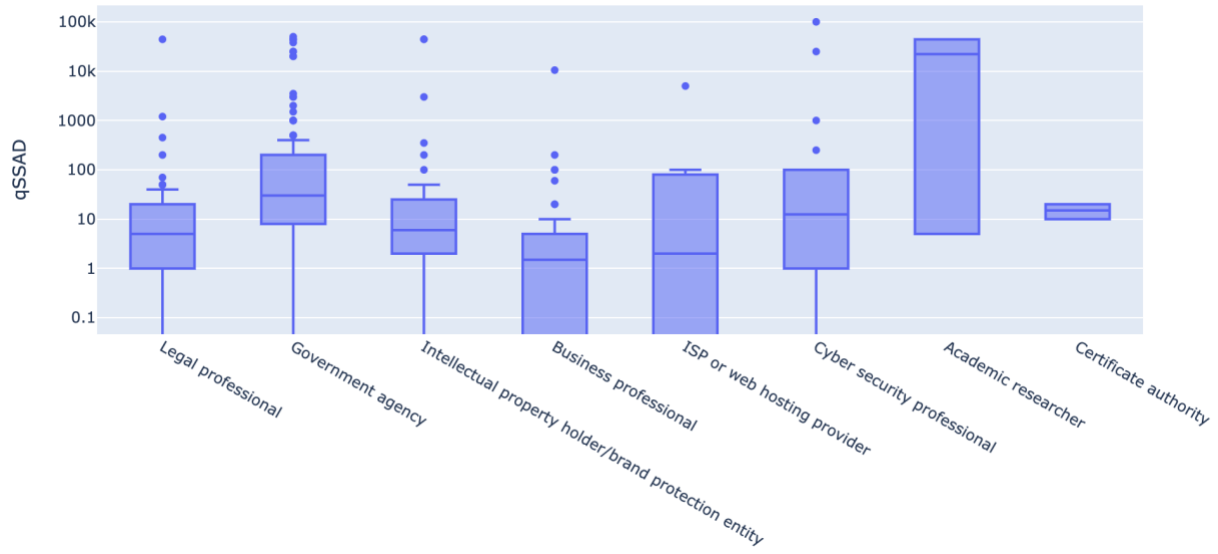

Figure A5-4. Community respondents estimated SSAD use by type of user.

- Some countries/jurisdictions, such as Europe and the United States, seem to predict a higher demand for the SSAD, though it's important to note that this may be due to the total number of respondents per territory.

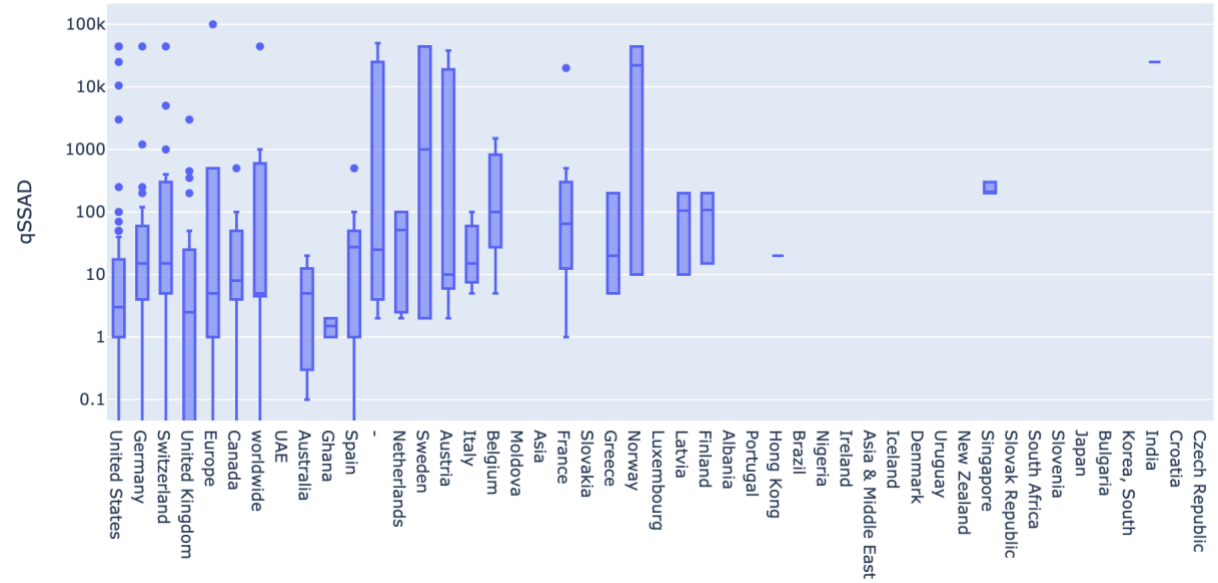

Figure A5-5. Community respondents estimated SSAD use by country.

- All factors that drive the usage of the SSAD timing/ efficiency (28.5%), ease of use (25.5%), accreditation and usage cost (24%), and results of requests (22.1%) seem to be roughly equally important to the community respondents. See **Figure A5-5**.

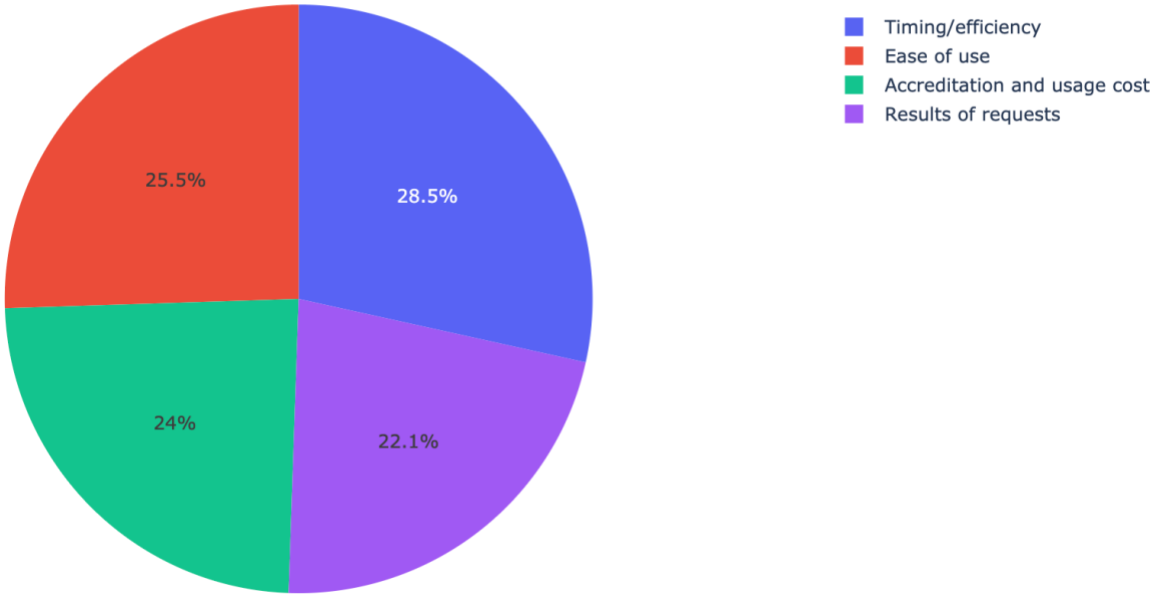

Figure A5-6. Reasons for SSAD use by community members.

- Participants identified the general public, social media companies, telecommunication operators, email providers, public safety advocates, and domain abusers (hackers/scammers) as additional groups that may be interested in using the SSAD to access nonpublic registration data.

Appendix 6 — Operational Design Phase Team Level of Effort

- The project team included approximately 30 staff members, representing every function within ICANN org, attending multiple weekly meetings, various subgroup meetings, and one-on-one discussions, to progress the ODP over ten months.
- The level of effort also included additional input from the ICANN org GDPR Steering Committee and nine members from the Board Caucus on GDPR / EPDP to participate in bi-weekly discussions.
- In addition to the main ODP team mentioned above, the project has benefited from the assistance of individuals outside of the project team, such as subject matter experts in market research, data analysis, and communications support.

.

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg