ICANN 75
ANNUAL GENERAL
KUALA LUMPUR

WHOIS Disclosure System Design Paper Summary Presentation

17 September 2022

Agenda

- What is the WHOIS Disclosure System?
- Design Highlights
- Overview: Request Intake Questions and Terms & Conditions
- User Interface Mockups
- Costs and Timeline
- Risks
- Alignment with Small Team
- SSAD vs WHOIS Disclosure System

WHOIS Disclosure System

WHOIS Disclosure System

Concept emerged from the ICANN Board/GNSO Council consultation on the SSAD-related recommendations from EPDP Phase 2.

- **Simplifies the process** for submitting and receiving requests for nonpublic gTLD registration data for both requestors and contracted parties.
  - Features for requestors to easily create and manage requests.
  - Features for registrars to effectively manage and process in-bound requests.
- **Cost-effective**
  - Simpler features allow system to be built quickly.
  - Less costly to build and maintain the system.
  - Utilization of existing ICANN systems.

System Design Highlights (1/4)

System Features

- Modeling off of CZDS
  - Using what's available within ICANN.
- System connects requestors and registrars.
  - Registries are not envisioned to be system users.
- System handles data requests for gTLD registration data.
  - Domains in ccTLDs and other non-contracted registries are out of scope.
- Email verification
  - No identity verification.
- Any communications between requestors and registrars takes place outside of the system.
  - i.e., Clarifying questions, additional documentation request, data disclosure, etc.
- No integration with registrars' systems.

System Design Highlights (2/4)

System Features

- Logging
  - System logs Request information
    - Request Type
    - Priority level (1-3)
    - Field elements requested
    - Jurisdiction where the nonpublic registration data will be processed
    - Registrar name associated with the domain subject
    - Legal basis for request
    - Existence of any supporting document for the request (subpoena, court order, or other legal process)
  - System logs Registrar's decisions
    - Change in priority level
    - Request approved/partially approved/denied
    - Disclosed data elements (i.e. name, email, phone #, etc)
    - The reason(s) for denial
  - Date and time stamps for all system activity
    - Request creation, status changes, response, etc.

System Design Highlights (3/4)

Other notable features

- Registrar participation
  - Registrars must provide "reasonable access" to registration data.
  - No specific policy or contract requirement for registrars to integrate with a WHOIS Disclosure System.
  - Org is exploring how to encourage participation, and will discuss with Small Team if implementation moves forward.
- ICANN-funded
  - No billing functions.

System Design Highlights (4/4)

Other notable features

- Privacy by design
  - Data minimization
  - No data will be retained for longer than necessary
  - Data will be kept secure (state of the art security) and accessible on a need-to-know basis only
- High-level design
  - Preliminary design only
  - May need to be amended based on technology requirements and best practices, as well as taking into account the principles of security and privacy by design

Overview: Request Intake Questions and Terms & Conditions

Overview: Request Intake Form

Questions

- Request type
- Jurisdiction(s) where data would be processed
- Third-party representation (if applicable)
- Purpose of request
- Request priority level
- Request legal basis (if applicable)
- Is there a subpoena, court order, other legal process?

Attestations and Terms & Conditions

Attestations

- Additional attestations must be provided for each request

Other Terms & Conditions and Privacy Notice

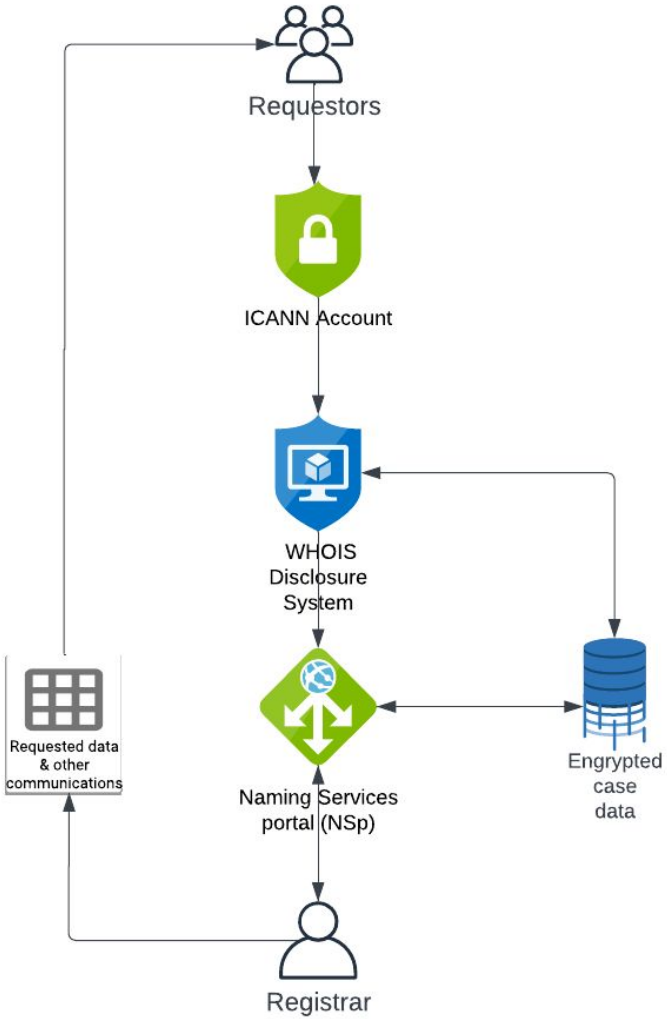
- Registrars must agree to NSp Terms & Conditions
- Requestors must agree Terms & Conditions for the WDS
- Requestors must agree and consent to the processing of their personal data and of data they process on behalf of third parties

Notes:

- *Registrars remain solely responsible for deciding whether or not to disclose the requested data*
- *Registrars may have additional terms and conditions that a requestor may need to execute before requested data is disclosed (outside of the system)*

Presentation of System Mockups

System Diagram



Cost and Timeline

+/- 9 months to develop

- Duration based on the full availability of required org resources.
- Start date unknown - ICANN Board and GNSO Council agreement on implementation needed.

Approx. $20k external costs to develop

- + Internal staff costs of approx. $1.7M
- Utilizing existing technology.

Funds

- ICANN's Supplemental Fund for Implementation of Community Recommendations (SFICR)

Approx. $70k to maintain (2-year maintenance)

- + Internal staff costs of approx. $1M (2-year maintenance only, no other operational costs included)
- + Contingency costs of $500k
- Maintenance to be 30% of the development cost.
- Contingency included.
- No other operational costs included (i.e., Global Support and Contractual Compliance) due to unknown usage and volume.

Notable Risks (1/3)

General Risks

- WHOIS Disclosure System may not produce actionable data.
  - Departure from SSAD means experience and learning gained from WHOIS Disclosure System may not directly inform questions about SSAD.
  - Requestors are free to continue requesting data directly from registrars, resulting in WHOIS Disclosure System collecting partial data.

Usage Risks

- Unknown demand for the WHOIS Disclosure System creates challenges to predict the impact of operating the system.
- Misconceptions about guaranteed data disclosure may deter requestors from using the system.

Notable Risks (2/3)

System Risks

- Vulnerable to malicious/nuisance submissions.
- No effective way to ban abusive users.

Registrar Participation Risks

- No contractual or policy requirements that specifically mandate registrar's interaction with a WHOIS Disclosure System.
  - Requestor experience may be inconsistent across registrars due to no service level agreement.
  - Inconsistent experience may drive up volume of complaints to Contractual Compliance.
  - Data (e.g., request processing time, approval/denial of data disclosure requests, etc.) gathered via the system could be inaccurate as it relies on manual reporting by registrars.
- No integration with registrars' systems may create manual work for registrars, driving participation down.

Notable Risks (3/3)

Legal Risks

- Increase potential liability for ICANN
  - System would require ICANN org to process a significant volume of personal data pertaining to requestors.
  - Operation of the system could make ICANN a litigation target.
- Update to Naming Services portal Terms of Use could raise concerns among CPs, which may delay implementation or reduce overall registrar participation.

Alignment with GNSO Small Team

Are we aligned with GNSO Small Team?

Design largely aligns with Small Team's Proof of Concept about what SSAD-related recommendations should be reflected in the *WHOIS Disclosure System.*

Exception: Contracted Party behaviors

No policy or contractual clause to mandate a specific behavior from registrars.

Alignment with GNSO Small Team

EPDP Phase 2 SSAD Recommendations	Small Team Proof of Concept	WHOIS Disclosure System
#1: Accreditation	Not relevant	Not available
#2: Accreditation of governmental entities	Not relevant	Not available
#3: Criteria and content of requests	Necessary	Contemplated
#4: Acknowledgement of receipt and relay of the disclosure request	Necessary	Contemplated
#5: Response requirements	Necessary	Contemplated
#6: Priority levels	Necessary	Contemplated
#7: Requestor purpose	Necessary	Contemplated
#8: Contracted party authorization	Necessary	Contemplated
#9: Automation of SSAD processing	Not relevant	Not available
#10: Determining variable SLAs for response times for SSAD	Necessary	Contemplated
#11: SSAD Terms and Conditions	Necessary	Contemplated
#12: Disclosure requirement	Necessary	Contemplated
#13: Query policy	Nice to have	Contemplated
#14: Financial sustainability	Not relevant	Not available
#15: Logging	Necessary	Contemplated
#16: Audits	Not relevant	Not available
#17: Reporting requirements	Necessary	Contemplated
#18: Review of implementation of policy recommendations concerning SSAD using a GNSO Standing Committee	Not relevant	Not available

WHOIS Disclosure System vs. SSAD

WHOIS Disclosure System vs. SSAD

	WHOIS Disclosure System		SSAD
Dev. Timeline	**+/- 9 months** • System development (requirements refinement, development, UAT, and launch)		**3 - 4 years** • IRT • RFPs • System development
Dev. Cost	**Approx. $20k** **(external infoSec & penetration testing)** • + Internal staff costs of approx. $1.7M		**Approx. $20M - $27M** • System development by vendors
Post-Launch Cost	**Approx. $70k** **(2-year license costs)** • + Internal staff costs of approx. $1M (2-year maintenance only, no other operational costs included) • + Contingency costs of $500k	**VS.**	**Approx. $14M - $107M** **(Annual Ongoing Operations)** • Operations outsourced • 7 functions vendors
Complexity	• **3** types of actors • **3** Subsystems • **2** Processes		• **8** types of actors • **8** Subsystems • **60** Processes
Fee Structure	**No Fee**		Accreditations/Identity Verifications: **$86 - $21 (low - high usage)** Requestor Declaration Verification: **$190- $160 (low - high usage)** Disclosure Requests: **$40 - $0.45 (low - high usage)**

Deviation from SSAD

- It does not include central or governmental accreditation authorities.
- It does not include accreditation of the requestors.
- It does not include identity verification of requestors.
- It does not include an abuse investigator.
- It does not include a billing function or any fees to the requester.
- There is no obligation or expectation of automated processing of certain requests by contracted parties.

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**

 @icann

 facebook.com/icannorg

 youtube.com/icannnews

 flickr.com/icann

 linkedin/company/icann

 slideshare/icannpresentations

 soundcloud/icann

Annex: Data Request Intake Form Questions

Data Request Intake Form Questions (1/5)

Q1: *Request Category

Selectable list: law enforcement, security researcher, computer security incident response team (CSIRT), cybersecurity incident response team (non-CSIRT), consumer protection, research (non-security), domain investor, IP holder, dispute resolution service provider, litigation/dispute resolution (non-IP), other (please explain)

Q2: If the category is "other", provide a description of the request category (the specific capacity in which the requestor is submitting this request).

Q3: Additional contact details: Postal Address

Q4: Additional contact details: telephone number

Q5: *Party representation: Select one of the options below:

- I am authorized to act on behalf of a third party in submitting this request.
- I am submitting this request on my own behalf.

Data Request Intake Form Questions (2/5)

Q6: Apply logic for each of the options selected above:

- If you choose “I am authorized to act on behalf of a third party in submitting this request” in Q5: In Q19, attach a statement (Power of Attorney) from the party you represent, that you represent them and their interests with regard to this request.
- “I confirm that I am authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.” (check box)
- If you chose “I am submitting this request on my own behalf” in Q5: no additional information is required.

Q7: *Identify the country or countries in which you or the party you represent will process the requested data if such data is provided to you by the contracted party, including jurisdictions in which any third party will process such data upon your behalf (including storage by a cloud service provider):

Selectable list of ICANN standard country code list. One or more jurisdictions can be selected.

Q8: *Provide full domain name subject to the request. The data entered must be a fully qualified domain name matching the format example.exampleTLD.

Q9: *List of data elements requested. (Can select multiple items)

Selectable List of data elements that may be requested: Registry Domain ID, Registry Registrant ID, Registrant Name, Registrant Org, Registrant Street, Registrant City, Registrant Postal Code, Registrant Phone, Registrant Email, Tech ID, Tech Name, Tech Phone, Tech Email.

Data Request Intake Form Questions (3/5)

Q10: *Identify your request priority level.

- Priority 1 - Urgent Requests: The criteria to determine urgent requests is limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation. For the avoidance of doubt, Priority 1 is not limited to requests from law enforcement agencies.
- Priority 2 - ICANN Administrative Proceedings: Disclosure requests that are the result of administrative proceedings under ICANN's contractual requirements or existing Consensus Policies, such as UDRP and URS verification requests. This priority assignment is limited to ICANN-approved dispute resolution service providers or its employees in the context of ICANN Administrative Proceedings.
- Priority 3 - All other requests.

Q11: If your request is a Priority 1 request, select the specific circumstance that applies:

Selectable List: imminent threat to life, imminent threat of serious bodily injury, imminent threat to critical infrastructure, imminent threat of child exploitation

Q12: If your request is a Priority 2 request, select the specific circumstance that applies:

Selectable List: UDRP verification request, URS verification request

Q13: *Provide a brief description of the specific issue the request is attempting to resolve.

Data Request Intake Form Questions (4/5)

Q14: *Has a Law Enforcement request for data such as subpoena, court order, warrant or any other form of legal request been issued requesting the disclosure of the requested data?

Yes/No

Q15: If the answer to 14 is "Yes", indicate if there is any specific date by which the contracted party must respond and attach a copy of the Law Enforcement request under Q19.

Enter date: mm/dd/yy

Q16: *Are you asserting a legal basis under which you would process the requested data pursuant to the European Union General Data Protection Regulation or other applicable law?

Yes/No

Q17: If the answer to 16 is yes, identify your asserted legal basis.

Selectable List:* GDPR Art. 6(1)a, data subject consent; GDPR Art. 6(1)b, contractual necessity; GDPR Art. 6(1)c, compliance with a legal obligation to which the controller is subject; GDPR Art. 6(1)d, processing is necessary to protect the vital interests of a data subject or other natural person; GDPR Art. 6(1)e, processing is necessary for a task carried out in the public interest, as set out in EU or EU Member State law; GDPR Art. 6(1)f, legitimate interests; other applicable law (non-GDPR) legal basis

Data Request Intake Form Questions (5/5)

Q18: If "other applicable law (non-GDPR) legal basis" is selected in Q17, identify the applicable law, including a section reference and explanation.

Q19: Attach any relevant documentation in support of the request, including any Law Enforcement request (subpoena, court order, etc.) identified above.

Affirmation:
A1: *I agree that the request is, to the best of my knowledge, complete and accurate, and that such request is submitted in good faith.

A2: *I affirm that any personal data received in response to this request will be processed and transferred in compliance with any applicable data protection law, and shall not be stored, transferred, or otherwise shared in contravention with any applicable data protection law. Where applicable data protection law requires a registrar to enter into contractual safeguards for the cross-border transfer of personal data, I agree that entering into such agreement with the registrar may be required before the registrar will disclose the requested data.