July 24, 2018

Goran Marby, President and CEO
Internet Corporation for Assigned Names and Numbers
via E-mail: goran.marby@icann.org

Dear Goran:

Thank you for publishing the below-referenced chart comparing ICANN's Unified Access Model discussion paper, the Accreditation and Access Model (v 1.5) and the Philly Special (v 2.0). This is a useful tool for comparing various proposals.

In addressing the Commercial Stakeholder Group at ICANN62, Theresa Swinehart invited corrections to the chart where necessary. Accordingly, we call your attention, for the purposes of clarification, to some changes to the chart that reflect the material in the existing Accreditation and Access Model and ask for those changes to be included in the posted chart.

This letter supplants our communication of 11 July. Thank you for your attention to this issue.

Sincerely,

ICANN Business Constituency
ICANN Intellectual Property Constituency

	Unified Access Model	**IPC/BC (v1.5)**	**Philly Special (v2.0)**
Eligibility			
Who would be eligible for continued access to WHOIS data via the Unified Access Model?	Defined set of user groups with legitimate interests who are bound by codes of conduct requiring adequate measures of protection. Users not part of an eligible user group would be required to request data from registries and registrars on an individual basis.	Defined groups of organizations or categories of organizations can gain access if they (1) require access for specific, legitimate and lawful purposes, and (2) are properly validated by 3rd party accreditor. Eligible user groups include (but not limited to): (a) Cybersecurity & OpSec Investigators; (b) Intellectual Property Owners and Agents; (c) Public Safety and Health Orgs; and Verification and Compliance Companies and Service Providers. (Model does not address	Authenticated users bound to measures of protection in an Access Agreement

		access for law enforcement.)	
Who would determine categories of eligible users?	Governments within the EEA would identify or facilitate the identification of categories of eligible user groups. Based on this ICANN org to engage with governments (via the GAC) to identify specific eligible user groups.	Defined by the community	Does not appear to be addressed by the model
How would eligibility requirements be developed?	For law enforcement authorities: individual governments would determine which authorities should be granted access. For private third parties: The GAC would be consulted on identifying relevant bodies with the appropriate level of expertise to approve users.	For Cybersecurity & OpSec Investigations: To be developed by security community For Intellectual Property Owners and Agents: To be developed by the IP community and associated organizations ~~leveraging staff and software of existing Trademark Clearinghouse (TMCH)~~ For Public Safety and Health Orgs: Not yet defined For Verification and Compliance Companies and Service Providers: Accreditation would be provided by an ICANN "Accreditation Review Panel", which would publish the criteria for access.	Does not appear to be addressed by the model
Process details			
Who would be required to provide access to non-public Whois data?	Both registries and registrars	Both registries and registrars	Only registrars (given privity of contract between registrar and registrant); "thick" registries to provide service only as a backup
What would be the overall process to	Option 1: authenticated user to be provided token/credential from	Decentralized process where users would be vetted by accreditation	Decentralized verification process to permit third-party organizations the

authenticate legitimate users?	centralized "credential provider" Option 2: authenticated user to be provided token/credential from "authenticating bodies"	authority. Upon accreditation, users would be given credentials to access WHOIS data	ability to verify legitimate users
What scope of data would be available to authenticated users?	Option 1: query-based access to full WHOIS data to level/scope of data consistent with identified legitimate purpose Option 2: query-based access to full WHOIS data	~~Does not appear to be addressed by the model~~ The full WHOIS record would be available	Does not appear to be addressed by the model
Would registry operators and registrars be required to provide access to all authenticated users?	Would be required to provide access consistent with legitimate purpose, and subject to applicable local laws.	Would be required to provide access consistent with legitimate purpose, and subject to applicable local laws. ~~Does not appear to be addressed by the model~~	Does not appear to be addressed by the model
Would the identity of those submitting Whois queries be known to registrants or other third parties?	The identity of users submitting queries would ordinarily be available to registrants and data protection authorities, and possibly to ICANN for compliance purposes	Query activity would be logged by the entity providing access to the WHOIS queries. Logged data would remain confidential by default and revealed only under legal justifications.	Queries using digital identities to be logged on permissioned distributed ledger maintained by registrar (or registry if relevant). Not clear from the model who may have access to the logs
Would the model incorporate transparency requirements?	Credential provider to maintain list of authenticated users Required to maintain logs of queries, unless logging not required pursuant to a court order	Mechanism would be provided for reporting to accreditation authority about over-extensive use, mirroring or other abuses. Third-party firm would randomly audit query logs for compliance	Ability to audit the system by legitimate users
Are there any fees associated with authentication process?	Requires further study	Yes. Model includes application and renewal fees sufficient to cover authentication process and onboarding. Model also includes renewal user fees, with further access continued upon successful payment.	Registrar (or registry if applicable) may impose micropayment on legitimate users accessing non-public WHOIS data, rather than registrants bearing cost of paying for privacy/proxy services

Would there be a process to review the effectiveness of the Unified Access Model?	Yes, to be reviewed at regular intervals to identify improvements	Does not appear to be addressed by the model	Does not appear to be addressed by the model
Technical Details			
Would there be a central repository of WHOIS data?	No. Registries and registrars required to maintain current requirements to operate a WHOIS service	No. Registries and registrars required to maintain current requirements to operate a WHOIS service	No. Registries and registrars required to maintain current requirements to operate a WHOIS service
What technical method will be required for registries and registrars to provide access to non-public Whois data?	Registration Data Access Protocol (RDAP)	Temporary solution: access to WHOIS data should be administered by ICANN, who would be responsible for delivering contracted parties information re: accredited entities/individuals Permanent solution: Possibly a federated authentication system for Registration Data Access Protocol (RDAP) based on OpenID Connect or use of Registration Directory Service Accreditation Authority (RDSAA) for Transport Layer Security (TLS) client authentication in conjunction with RDAP	Registration Data Access Protocol (RDAP)
What technical method would be used to authenticate users?	Relies on a system of tokens and/or certificates as the technical method for identifying authenticated users	In the short-term, a whitelist of authenticated users should be operated by ICANN and administrated via the existing RADAR system. Contracted parties validate requesting IP address with the centralized list of whitelisted IP addresses, and are then able to deliver access to single record queries and automated access via port 43.	Authenticated user assigned digital identity credentials. Digital identity credentials used to securely access RDAP platform using multi-factor authentication.

		A similar approach should be developed and implemented for volume WHOIS queries until such time that RDAP is implemented.	
Codes of Conduct / Safeguards			
Would there be multiple Codes of Conduct?	Multiple codes of conduct, with some common safeguards across codes of conduct	Model appears to include a single code of conduct. Access would be provided to approved parties under the approved code of conduct or accreditation / certification mechanism	Does not include codes of conduct, but rights and obligations for access governed by Access Agreement between registrar and authenticated user, along with registrar's Terms of Use and Privacy Policy
How would Codes of Conduct/safeguards for accessing data be developed?	Standard safeguards: to be developed in consultation with the GAC and European Data Protection Board Safeguards specific to eligible user group: to be developed by the authenticating body	Does not appear to be addressed by the model	Safeguards for accessing data would be established in an Access Agreement, which is under development as part of the model
What types of safeguards would be included in Codes of Conduct?	(1) Limitations on use of data; (2) Procedures for accessing data; (3) Security measures; (4) Limitations on onward transfers of data; (5) General data protection obligations of the data controller; (6) Fair and transparent processing requirements; (7) Other safeguards/public policy considerations	(1) Limitations on use of data; (2) Procedures for accessing data; (3) Security measures; (4) Limitations on onward transfers of data; (5) General data protection obligations of the data controller; (6) Safeguards addressing data misuse and penalties for misuse.	Safeguards for accessing data would be established in an Access Agreement, which is under development as part of the model
What mechanism would be used to require compliance of Codes of Conduct?	Model contemplates an agreement or other method to bind user to comply with code of conduct	Model contemplates binding terms requiring parties accessing non-public WHOIS data to put in place appropriate internal controls/safeguards for accessing data	Legitimate user required to execute an Access Agreement subjecting the user to Alternative Dispute Resolution proceedings initiated by data subjects and registrar (or registry) seeking to revoke access

			due to documented abuse Legitimate user required to provide financial instrument (e.g. letter of credit) to ensure data subject could be made whole upon successful dispute resolution proceeding
Who would monitor and enforce compliance with the Code of Conduct?	Complaints re: breach of code of conduct (e.g. unauthorized access or improper use of data), to be directed to authenticating body Complaints re: registry/registrar performance of Whois service, to be directed to ICANN compliance	Complaints re: accuracy to be addressed by sponsoring registrar Complaints re: performance of Whois provider, to be directed to ICANN compliance Complaints re: unauthorized access or improper use of data to be relayed to the authenticating agency	Complaints handled through Alternative Dispute Resolution (ADR) proceedings. European Data Protection Board could help establish best practices or certification frameworks for ADR proceedings.
Other Elements			Registrars (and registries) to implement model through their own initiative