**BC ACCREDITATION PRINCIPLES**

**Eligibility**

The BC envisions access granted to various eligible entities that include, but are not limited to:

* Cybersecurity and OpSec Investigators
* Intellectual Property Owners and Agents
* Verification and Compliance Authorities

Note: that law enforcement agencies are not listed here, as these will be addressed by the GAC representatives on the EPDP.

**Determining eligibility**

Eligible entities are those with legitimate purposes for access to non-public WHOIS data, in compliance with GDPR. Final determination of eligibility is made by an ICANN-approved accreditation review authority.

**Authentication process**

All eligible entities must:

* Have a specific and delineated purpose for their access to and use of non-public data
* Represent that access to and use of non-public data is for a legitimate and lawful purpose and its processing will not be incompatible with the purpose for which it is sought.
* Comply with applicable laws (e.g., GDPR) and terms of service to prevent abuse of data accessed
* Be subject to graduated penalties, and ultimately de-accreditation if they are found to abuse use of data
* Be subject to penalties under applicable laws (e.g., GDPR)
* Submit an application with verifiable contact details, covering the information required under Recommendation 18 of the EPDP Phase 1 Report.
* Undergo validation by an ICANN-approved agent (similar to the services offered by certificate authorities or those offered by Deloitte for the trademark clearinghouse)

Once the eligible entity successfully completes the above steps, the ICANN-approved accreditation authority issues one of three decisions:

Application is accepted and the applicant is issued credential

- Or –

Applicant is returned with questions

- Or –

Application is rejected

**Fees**

* All applicants must pay a to-be-determined non-refundable application fee proportional to the cost of validating an application.
* Rejected applicants may re-apply, each time paying the fee.
* Fees are to be established by the accreditation authority
* Accredited parties must renew their accreditation annually.
* Application and renewal fees should scale with the number of users for each accredited entity.

**Accreditation procedure**

The accreditation approach for this BC proposal encompasses three (3) types of “Accreditation Categories”:

* Regular Access;
* Special Access; and
* One-Time Access.

Accreditation would be provided by an ICANN-approved accreditation authority. The authority would publish the criteria for access, which would encompass the three accreditation categories.

* Accredited parties must renew their accreditation annually.
* Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority.
* User fees are due and payable upon the date of start of service, again on date of renewal, and with further access conditioned upon successful payment.
* Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation.
* The accreditation authority reserves the right to update what credentials or other material are required for accreditation.

**Logging**

* The query activity of all accredited entities will be logged by the entity that provides access to the WHOIS queries.
* Logs will include accredited entity, purpose, query, and date.
* Logs must be retained for a two-year period in a machine-readable format and be kept up-to-date with each new query.
* Logged data will remain confidential by default and can be revealed only under legal justifications (revelation could, for example, compromise law enforcement investigations).
* In the event of an audit or claim of misuse, logs may be requested for examination by an accreditation authority or dispute resolution provider.
* Logs should be further available to data protection authorities and ICANN for auditing. Each query must be mapped to a purpose that is applicable.

**Auditing**

* A third-party firm should randomly audit a small sample of query logs for compliance with terms and conditions funded by accreditation and renewal fees.
* A contracted party’s logs for access may be matched to an accredited entity’s logs by a third party to discern misuse/abuse.
* Query logs should cite purposes of access, which must be tied to a legitimate and legal use for each accredited user’s use case.
* Audits will be conducted by a third-party bonded company, and logs are to be delivered with identity of the log origin tokenized or anonymized so that the auditing organization cannot see and thus risk identifying methods of an accredited party.

**Complaints**

* Complaints regarding accuracy of data will be addressed directly to the domain name’s sponsoring registrar for resolution.
* Complaints regarding performance of underlying WHOIS providers will be directed to ICANN’s Compliance Department, which will address the matter with the appropriate registrar or registry operator, according to the terms of the contract.
* All other available remedies (e.g., filing data accuracy complaints) are available to all appropriate parties.
* Complaints regarding unauthorized access to, or improper use of, data will be relayed to the accrediting agency for appropriate remedial action.

**Data access**

* Accredited data access is to be provided for legitimate uses either for single record queries or automated multiple queries and responses for analysis.
* Accredited access shall not be rate-limited or otherwise restricted except where the requester poses a demonstrable threat to a properly resourced system.
* Data may be stored by accredited users for analysis and collection of case data.
* Per GDPR, any accredited user will be expected to only process the personal data that it needs to process in order to achieve its processing purposes. They will be obligated to minimize the number of queries they make to those that are reasonably necessary to achieve the purpose.
* Accredited entities will be required to follow the safeguards from the Acceptable Use Building Block.

**Types of Accreditation**

Regular Access Accreditation is for companies who require access to the non-public WHOIS for a legitimate purpose on an ongoing and regular basis, and which need to submit higher volume requests.

The evaluation of an applicant for Regular Access Accreditation would involve, *inter alia*, a rigorous inspection and evaluation of:

* its identity and supporting documents such as Articles of Incorporation, licenses, regulatory and governmental filings;
* letters of reference from credible sources familiar with the legitimate purposes and reputation of the applicant;
* a thorough and detailed description of its business, identification of the officers, directors, and shareholders, financial summaries or statements; and
* a detailed request setting out the basis for the legitimate purpose being claimed.

The accreditation authority would make a determination as to whether the applicant qualified based upon its level of ascertainable trustworthiness:

* financial stability;
* reputation;
* length of its establishment;
* qualifications of management and procedures for compliance and governance; and other factors which identify the applicant as an entity qualified and deserving of Accreditation; and
* other factors which identify the applicant as an entity qualified and deserving of Accreditation

The overriding criteria however, would be that the applicant has an established and credible legitimate purpose for requiring ongoing and regular access, such as those entities that are addressed in the BC 1-3, 9 Use Cases.

Applicants for Regular Access Accreditation would be required to post a bond or evidence of insurance to secure their obligations, and may be subject to higher accreditation fees.

B. Special Access Accreditation

Special Access Accreditation is for those persons who require access to the non-public WHOIS database on an ongoing but intermittent basis for legitimate purposes.

The evaluation of an applicant for Special Access Accreditation would involve:

* inspection of its identity and supporting documents such as Articles of Incorporation, licenses, Law Society or Bar admissions, accounting licenses, and/or regulatory and governmental filings;
* letters of references;
* a description of its business;
* identification of its officers, directors, shareholders, partners, or other ownership structure;
* a detailed request setting out the basis for the legitimate purpose being claimed; and
* The accreditation authority would make a determination as to whether the applicant qualified based upon;
* its level of ascertainable trustworthiness:
  + reputation;
  + length of its establishment;
  + qualifications of management and personnel;
  + procedures for compliance and governance; and
  + other factors which identify the applicant as an entity qualified and deserving of accreditation. The overriding criteria however, would be that the applicant has an established and credible legitimate purpose for requiring ongoing and regular access.

C. One-Time Accreditation

One-Time Accreditation is for those persons who require access to the non-public WHOIS on an ad hoc or one-time basis for a specific and limited legitimate purpose.

Applicants for One-Time Accreditation would provide the following as part of their application to the accreditation authority:

* Notarized government issued photo identification;
* A detailed description of the basis for the request for one-time access, together with supporting documentation; and
* Any credentials, licenses, or other documents supporting the specific requirements and qualifications of the applicant.

**De-Accreditation**

* Accredited entities will be subject to graduated penalties, and ultimately de-accreditation if they are found to abuse use of data.
* De-Accreditation will occur when the accreditation authority determines that the Accredited person has materially breached the conditions of its Accreditation based upon either; a) a third-party complaint received; b) results of an audit or investigation by the Accreditation Review Panel; or c) otherwise for any misuse or abuse of the privileges afforded.
* De-accreditation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Review Panel. De-accreditation procedures will be on reasonable notice to the Accredited person who shall have the right to a hearing and of appeal.
* Deaccreditation does not prevent the requestor from submitting future requests under Recommendation 18 of the Phase 1 Report, but that they will not be accredited, and thus will be subject to delays, and manual processing.
* In the case of Regular Access Accredited parties, in the case of de-Accreditation, any posted bond may be forfeited in whole or in part, and other additional financial penalties may be assessed.