

# ALAC Comment on NIS2 to be submitted to the European Commission

## DRAFT 14 March 2021

[This is a more complete and readable version of the formal 4000 character submitted comment.]

This comment is being submitted on behalf of the At-Large Advisory Committee (ALAC) of the Internet Corporation for Assigned Name and Numbers (ICANN).

The ALAC is responsible for representing the interests of individual Internet users within ICANN. As such the ALAC and the At-Large Community which it represents has a great interest in ensuring that individual Internet users can go about their online activities with safety and security.

As such, the European Commission's Proposal for a revised Directive on Security of Network and Information Systems (NIS2) is of great interest to the ALAC and the ALAC strongly supports this initiative. NIS2 has the potential for significantly improving individual Internet user's ability to use the Internet free of the threats that now confront them regularly. NIS2 will help address the increasing illegal activities including fraud, phishing, cyber-attack and malware. As stated in NIS2 recital 15, "Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend."

However, it is the view of the ALAC that as the proposal is currently written, there are a number of gaps that will not allow it to fulfil its intended function. The ALAC is specifically concerned that Article 23 on *Databases of domain names and registration data* and related sections need a number of refinements to ensure that it meets its intended goals.

For the generic TLD (gTLD) overseen by ICANN, the "registration data" is collected and generally held not by registries but by what Article 23 refers to as "entities providing domain name registration services" and what recital 61 parenthetically refers to as "so-called registrars". To ensure that Article 23 has its desired effect, it is necessary to ensure that all of the entities involved in providing domain name registration services are clearly and unambiguously cited in NIS2. Moreover, it is important that their responsibilities are similarly clearly and unambiguously stated.

Within the gTLD space, registrars are the prime entities that offer domain registration services, but they are not the only such entities:

- For .com and other TLDs, and due to recent ICANN policy, potentially for many other TLDs, the registration data is not held by the registry, but by the registrar. This comprises the vast majority of all gTLD registrations.
- Many registrars have "resellers" and it is these resellers that interact with the registrant.

- Moreover, resellers may themselves have resellers. These 2<sup>nd</sup>-order resellers have no direct link to or contract with the registrar and in fact, the registrar may not even be aware of them. There is no limit to the depth of this reseller chain.
- Some or all of the registration data may never be stored by (or even presented to) the registrar. It will be held by a privacy or proxy provider. A privacy provider will allow the name of the real registrant to be stored in the domain registration data, but not any contact information. A proxy provider will not pass on either the name of the real registrant or their contact information. A privacy/proxy (P/P) provider may be an affiliate of the registrar or reseller, or a completely separate entity.
- For a P/P registration made through a reseller only the reseller or the P/P provider can verify the accuracy of the registration data.

The following comments are based on the public NIS2 documents issued by the Commission as well as the 26 February 2021 Briefing where EC representatives presented an overview of NIS2 to the ICANN community.

## **ARTICLE 2: SCOPE**

Article 2 ensures that all TLD registries, regardless of size, are subject to NIS2. However, Article 2 makes no reference to registrars, resellers or P/P providers, many of who satisfy the Commission definition of micro or small enterprises (fewer than 50 persons and annual turnover of less than EUR 10 million)

It is essential that NIS2 explicitly covers all of the players in the domain registration process.

## **ARTICLE 4: DEFINITIONS**

It is critical that all of the known players in the domain registration process be identified and defined. This clearly includes registrars but should also reference resellers and P/P providers, either as separate definitions or explicitly within the registrar definition.

It is understood that this list may not be exhaustive, but it is essential to identify those who are known to play significant roles.

## **ARTICLE 23: DATABASES OF DOMAIN NAMES AND REGISTRATION DATA**

**Accuracy:** Section 1 calls for the collection and maintenance of accurate and complete registration data. Section 2 ensures that the Section 1 data be usable to identify and contact the domain name holder. This clarity is appreciated. Nevertheless, there is a persistent belief among some privacy advocates and registrars that the data subject is the sole judge of “accuracy” and that if the data subject is satisfied with its contact information, no further efforts need to be taken. Since it is known that some domain name registrants do not wish to be contacted, this can result in an untenable situation.

Anything that can be done to ensure that true identification and contactability is the required goal, the more likely that this directive can be followed. Specifically, that it is the obligation of the registrar or their agents to verify accuracy and contactability.

**Penalties:** It is unclear to what extent penalties apply to infractions of Article 23. During the Briefing, the question was asked but the only definitive answer offered was that they were not subject to specified maximums. This is linked to the status of entities listed in Annexes I and II on Essential and Important Entities. If there are not clear and dissuasive penalties, then Article 23 becomes meaningless.

**Non-personal Data:** Section 4 requires that all registration data that is not personal data must be published without undue delay. Registrars have expressed concern that they have no way to ensure that contact details are not in fact those of a natural person and therefore will not risk publication. This issue must be addressed.

**Applicability to registrars and associated entities:** The documents mention registrars and during the Briefing, it was stated that the intent was to include such entities as resellers and P/P providers. However, if it is not explicit, there is no guarantee that such entities will be included in national laws nor in ICANN policies that are developed based on NIS2. See also comments on Annexes I and II.

**Undue delay:** Article sections 23.4 and 23.5 make reference to “without undue delay”. Although the ALAC understands the EC desire that NIS2 remain high level and leave specificity to the Member States, the potential for misinterpretation here is too great. As an example, in the draft ICANN policy for release of information (as described in Article 23.5), for a URGENT request (those involving imminent threat to human life, critical infrastructure or child exploitation), the typical response allowed is 1 business day (limited to 3 calendar days). Other types of request allow for a mean (not maximum) response time of up to 10 business days (between 2 and 3 weeks).

**Publication:** Article 23.4 calls for the publication of specific registration data. The form of publication must be specified, presumably via publicly accessible Internet access and without charge.

## CHAPTER VI: SUPERVISION AND ENFORCEMENT

Registries are classified as Essential entities and are therefore subject to the appropriate terms of Articles 28-34. Because the enterprises responsible for the registration of domain names are not so listed, these critical regulations do not cover them.

### ANNEX I/II: ESSENTIAL/IMPORTANT ENTITIES

Registrars, resellers and Privacy/Proxy providers must be included as either essential or important services. If they are not, they are not subject to regulations such as those described under Articles 29 and 30 on supervision. In the opinion of the ALAC, these enterprises should be classed as essential entities just as TLD registries are. It is the registrars, resellers and P/P providers that collect all of the data and are responsible for storing and releasing it in almost all cases.

During the Briefing, it was stated that since many registrars run authoritative DNS servers, they were implicitly covered. The ALAC notes that running such a server is a convenience to its customers and is by no means a requirement for a registrar. Moreover, that service could be outsourced and it does not apply to resellers nor P/P providers. Accordingly, this is no substitute for explicitly identifying these entities as being critical in their own right.

## SUMMARY

The ALAC appreciates the NIS2 initiative in regard to ICANN-related services and specifically thanks the European Commission for this opportunity to submit comments. NIS2, with appropriate enhancements as described in this comment, has the potential to greatly improve Internet security and the ALAC looks forward to its being adopted by the European Parliament and acted on by the Member States.