ICANN BUSINESS CONSTITUENCY

INPUT TO MEP MAYDELL, ITRE SHADOW RAPPORTEUR FOR THE "NIS2" DIRECTIVE

ENSURING WHOIS DATA ACCESS THAT SUPPORTS CYBERSECURITY, LAW ENFORCEMENT, AND RESPONSIBLE BUSINESS ON THE INTERNET

September 3, 2021

Dear Ms Maydell:

On behalf of ICANN's Business Constituency (BC), the representative group of worldwide business and commercial Internet users, we would like to thank you for the important work that you, as Shadow Rapporteur, and the entire ITRE Committee are undertaking with respect to the proposed directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, i.e., the "NIS2" Directive. We are writing to convey support for many of the amendments to NIS2 developed to date and strengthened by both the ITRE Committee's Draft Report and the IMCO Committee's Opinion. We recognize this valuable effort to restore and sustain access to domain name registration ("WHOIS") data, which is vital to cybersecurity in the EU and beyond.

The BC is the voice of commercial Internet users within ICANN, the multistakeholder group and nonprofit organisation responsible for coordinating a stable, secure, and unified global Internet. We represent the interests of small, medium, large and multinational enterprises as users of the domain name system (DNS).

We very much support your and your colleagues' work thus far. Your commitment to producing a strong revised directive will ensure a more secure Internet for citizens, consumers, and business. It has been made clear through the amendments process that you and many other MEPs on the ITRE committee are keenly aware of the importance of efficient and effective access to accurate and complete WHOIS data in the context of cybersecurity. At the same time, strong privacy protections for personal data must be in place and adhered to, and the BC will only stand behind policies and practices that strike a proper balance between the individual right to privacy and the safeguards necessary to ensure public safety and legal obligations are met.

As it stands, the policies and practices that today determine access to WHOIS data simply "do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars, and those protecting the public from harms associated with bad actors seeking to exploit the domain name system." That was the conclusion of our colleagues on ICANN's Government Advisory Committee (GAC), where the EU is represented by the European Commission. It is a view we share of a situation that we are committed to change.

With that project in mind, we would like to take the opportunity in this letter to discuss five critical components of the NIS2 proposal where great progress has been made, and to submit our support for specific amendments or propose additional changes to the provisions that will go a long way to help ensure that WHOIS data access once again supports cybersecurity and law enforcement on the Internet.

I. **Access to and disclosure of certain WHOIS data is in the public interest and it is also necessary for compliance with a legal obligation**

II. **Domain name registration data must be *accurate* and *verified***

III. **Specific timelines are necessary when it comes to the availability of public WHOIS data and the disclosure of non-public data in response to requests from legitimate access seekers**

IV. A definition for *legitimate access seekers* would be helpful

V. All actors with a role in the domain name registration supply chain should be in scope

The Summary Analysis attached provides specific proposals and justifications supporting each of the five components. This is followed by additional background and data on the current lack of access to domain registration information and the impact it is having on cybersecurity. The letter concludes with a detailed justification for the proposals outlined in component I, which advocate for amendments to the draft directive that will make it clear that the processing of WHOIS data, including critical personal data elements, is in the public interest and can also be necessary for compliance with a legal obligation, including lawful disclosure requests from legitimate access seekers.

We respectfully submit these proposals with a sincere interest in strengthening the NIS2 directive and specifically to ensure follow-through of intent when it comes to reforming and restoring access to WHOIS information.

BC representatives are available to discuss with you the input below and are happy to do so at your convenience. Thank you for your time and attention.

On behalf of the Business Constituency,

Mason Cole
Chair

Summary Analysis and Support For Key Proposals In Committee Reports

I. Access to and disclosure of certain WHOIS data is in the public interest and is also necessary for compliance with a legal obligation

In order to achieve the shared objective of reliable and effective access to WHOIS information that will strengthen cybersecurity and protect against a litany of online harms, the directive should make it clear that the processing of WHOIS data, including critical personal data elements, is in the public interest. We also support the creation of a legal obligation to clarify that such data should be promptly disclosed to legitimate access seekers. [A detailed explanation and justification for these proposals begins on p9.]

- **We propose an additional subparagraph to Article 23** that will clearly establish the processing of critical WHOIS registration data elements as serving the public interest, as provided for in Article 6(1)(e) of the GDPR:

  (6) "Domain name registration data serves the public interest as provided for in Article 6(1)(e) of the GDPR; accordingly, Member States shall ensure that a natural person registrant's name, verified email address - and postal address, as appropriate to establish jurisdiction - are disclosed when requested for legitimate purposes."

- We propose an additional amendment to Recital 69 that will clarify the intent of the directive when it comes to WHOIS data and establish the disclosure of WHOIS data to legitimate access seekers as a legal obligation, therefore relieving registrars and registries of balancing test duties under GDPR:

  (69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by essential and important entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services, **as well as access to domain name registration data by legitimate access seekers,** is necessary to comply with a legal obligation under this Directive and constitutes a legitimate interest of the data controller concerned, as referred to in point (c) paragraph 1, and point (f) paragraph 1 respectively of Article 6 of Regulation (EU) 2016/679

II. Domain name registration data must be *accurate* and *verified*

WHOIS records today are frequently inaccurate, as bad actors often intentionally provide erroneous data. Making matters worse, the entities providing domain name registry and registration services are not required to verify the accuracy of WHOIS data.

The NIS2 proposal contains a number of essential provisions that require the collection and maintenance of **accurate** WHOIS data, and a number of proposed amendments from both the ITRE and IMCO committees will strengthen these provisions by adding the requirement that registries and registrars **verify** domain name registration data and proactively work to correct inaccurate or incomplete data. This language in the directive is an essential step toward rendering WHOIS data reliable, and thus usable, and recognizes its important role in cybersecurity.

- We support amendments to Article 23 Paragraph 1 that add a verification requirement such that Member States are empowered to ensure that TLD registries and the entities providing domain name registration services for the TLD***,*** shall collect***, verify*** and maintain accurate and complete domain name registration data.

- In order to bring additional clarity to the accuracy requirement and the duties associated with it, we note the additional language to **Article 23 Paragraph 3 as proposed in IMCO Compromise Amendment (CA) 20**

and respectfully propose a modified amendment **that inaccurate or incomplete data should be corrected without delay.**

IMCO CA 20 on Article 23 Paragraph 3
Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the ***database infrastructure includes*** accurate***, verified*** and complete information***, and that inaccurate or incomplete data should be corrected*** ~~***or erased by the registrant***~~ ***without delay***. Member States shall ensure that such policies and procedures are made publicly available.

- We support Amendment 181 proposed by you and your ITRE Committee colleagues that conveys the importance of maintaining accurate and complete WHOIS data that can also be ***verified***. We greatly appreciate and support the additional language in the amendment that highlights the importance of **third-party rights** to cybersecurity.

III. Specific timelines are necessary when it comes to the availability of public WHOIS data and the disclosure of non-public data in response to requests from legitimate access seekers

The requirement to make registration data for legal persons publicly available within 24 hours of domain name registration is very encouraging. In today's scenario, such data often is intentionally concealed, with requests for access ignored, and the experience of law enforcement and legitimate access seekers tells us that language in the directive that specifies a timeline (in *hours*) is required in order to clarify the importance of this data and the need for its timely publication.

With these goals in mind, we would also like to bring to your attention the potential for certain interpretations of the word "publish" in Article 23 Paragraph 4 of the draft directive. Likewise, we highlight the fact that, to be accurate, informative, and useful, domain name registration data needs to be continuously available and updated to reflect changes to the registration, which occur regularly.

- We support proposed amendments that include a 24 hour timeline for publication and propose additional language below that builds on the **IMCO Committee's CA 20 to Article 23 Paragraph 4**:

  Member States shall ensure that the TLD registries and the entities providing domain name registration services ***make continuously publicly available***, ***without restriction and*** without undue delay ***and in any event within 24 hours*** after the registration of a domain name ***and after any changes to the registration of that domain name***, ***all*** domain registration data ***of legal persons as registrants***.

The need for a timeline to ensure a response to requests for non-public registration data is just as important and we support the many proposals in committee reports that include a requirement to provide, within 72 hours, registration data based on a legitimate request. As you may know, registrars and registries currently are not bound by such a deadline, and in policy discussions have proposed far lengthier timelines that would impair or even debilitate many cybersecurity investigations.

Based on experience it will be necessary to clarify that, in response to such a request, TLD registries and entities providing domain name registration services *disclose* the requested data within 72 hours. A requirement to simply "reply" to such requests is not likely to yield actionable information for law enforcement or other legitimate access seekers.

- We support **ITRE Amendment 507** and respectfully propose additional language to the following section of **Recital 59** that will clarify the need for disclosure:

(59) … Member States shall ensure that the TLD registries and entities providing domain name registration services ~~reply~~ **disclose specific domain name registration data within 72 hours** to all **lawful and duly justified** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

IV. A definition for *legitimate access seekers* would be helpful

The Commission's draft directive and subsequent EP committee reports clearly state that cybersecurity is enhanced when certain stakeholders have access to critical data, including WHOIS data. The term 'legitimate access seekers' is used throughout the directive in reference to these types of requests for data, but it would be helpful to define it.

- We support ITRE Amendment 256 that proposes an accurate and useful definition:

  (15a) 'legitimate access seekers' means any natural or legal person, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CSIRTs, CERTs, providers of electronic communications networks and services, and providers of cybersecurity technologies and services, seeking DNS data upon a justified request on the basis of Union or national law for the purposes of preventing DNS abuse, detecting and preventing crime and fraud, protecting minors, protecting intellectual property, and protecting against hate speech;

- We are also supportive of the definition for legitimate access seekers included in **ITRE Amendment 183 (to Recital 60)** and we likewise appreciate the language that details the value to cybersecurity and criminal enforcement that results from timely access to domain name registration data for legitimate access seekers.

V. All actors with a role in the domain name registration supply chain should be in scope

There are a number of different service providers that could play a role in collecting and maintaining WHOIS data beyond the TLD registry. You and your colleagues on the ITRE Committee clearly recognized the important role registrars play. Likewise, privacy or proxy registration service providers, and domain brokers or resellers, are among the other entities that will need to be accountable to the key WHOIS provisions being developed in NIS2.

- We do not want to limit the scope of the directive and therefore respectfully encourage the retention of Commission language referring to "entities providing domain name registration services for the TLD" **throughout Article 23**.

- In order to highlight some of the specific entities that play a role in the domain name registration supply chain, we support the additional language proposed in the IMCO CA 51 on Recital 61:

  In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services ~~for the TLD~~ ~~(so-called registrars)~~ ***(including services provided by domain name registries and*** registrars***, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names***) should collect and guarantee the integrity and availability of domain names registration data.

Background and data on current lack of access to domain registration information

Since the GDPR came into effect in May 2018, cybersecurity and rights protection work has become far more difficult and less effective due to the lack of access to WHOIS data. This is due primarily to exposed gaps in ICANN policy that enable and propagate misinterpretations and misapplications of the scope and rules of the GDPR. Yet after more than three years of ICANN process work, there is no sign of a workable system for the efficient and effective request, processing, and disclosure of WHOIS data.

A June 2021 survey of nearly 300 cybersecurity experts by the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG) highlighted the futile reality for law enforcement and other legitimate access seekers requesting basic information on domain name registration and hoping in vain for some type of action by ICANN to change this reality. The report concluded:

- "94% of our respondents report that redaction [of WHOIS data] impairs their ability to investigate relationships between malicious domains and actors."
- "Two-thirds of our respondents indicate that their ability to detect malicious domains has decreased."
- "The solutions currently discussed at ICANN would not meet the needs of law enforcement and cybersecurity actors in terms of timelines."
- "Changes to WHOIS access following ICANN's implementation of the EU GDPR . . . continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks."

With its focus on improving cybersecurity throughout the EU, the NIS2 Directive presents an important and relevant opportunity to address the serious concerns and shortcomings described above. The recognition of the importance of WHOIS data to this objective was made clear in the draft ITRE Report's Explanatory Memorandum, where your committee's Lead Rapporteur referred to WHOIS data as "the authoritative record of domain ownership," and "the only viable means to obtain the information necessary to identify criminal actors, track threat actors, prevent harms and protect the online ecosystem."

The current reality is in stark contrast to this statement: according to one estimate, 86.5% of domain registrants cannot be identified via WHOIS -- up from 24% before GDPR went into effect.[1]

This is an environment where there is a shortage of reliable data and legal clarity is lacking. And now, at least one registrar has begun to charge fees for WHOIS access, beginning at $750 for five lookups and an additional $50 for every additional lookup request.[2] These charges apply to law enforcement officials as well -- consider the scale of requests law enforcement will require, based on data from the M3AAWG report, and the chilling effect of predatory lookup fees (emphasis added):

> "To respond to cybercriminals that leverage bulk buying and bulk resource use, **investigators query WHOIS data constantly and at all times** to detect patterns…"
>
> "To fight crime and abuse, large datasets are particularly powerful: investigators and analysts can use them to map out and then dismantle criminal attack infrastructures, while bulk data enables blue teams to protect their networks. **For this data-driven approach to work, however, high-volume, realtime access to WHOIS records is essentially required**."[3]

[1] Interisle Consulting Group Whitepaper, "WHOIS Contact Data Availability and Registrant Classification Study," January 21, available at: http://www.interisle.net/ContactStudy2021.html

[2] See "Tucows Tiered Access Compliance and Operations System Terms of Service," available at: https://tieredaccess.com/terms

[3] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf at page 5

ICANN policy, or lack thereof, has instigated and is now sustaining a fragmented and unpredictable system, wherein each individual domain name registrar or registry weighs the interests of legitimate access seekers against the data privacy/fundamental rights of the data subject, i.e. the domain registrant, in accordance with Article 6(1)(f) of the GDPR. Please note that this ICANN policy is being applied equally to legal and natural persons' data, despite the scope of the GDPR. While fully supportive of data protection rights, we note that such "balancing tests" by these DNS operators ignore other fundamental rights (such as the protection of intellectual property in Article 17 of the Charter on Fundamental Rights) and public interest needs of law enforcement, consumer protection and cybersecurity professionals.

The BC and other stakeholders active in ICANN's multistakeholder community, including the Governmental Advisory Committee (GAC), where the EU is represented by the European Commission, have repeatedly warned, through public submissions, that the vital public interest and business needs of professionals engaged in cybersecurity, consumer protection, law enforcement, and intellectual property protection are consistently disrupted or simply ignored as a result of ICANN's and registrars' and registries' misapplication of certain important privacy protections created by the GDPR.[4]

The BC has always expressed, and continues to put forward, strong support for privacy protections for personal data and is invested in the development of ICANN policies that strike the correct balance between the individual's right to privacy and safeguards for law enforcement and other legitimate interests. But we agree with the GAC, which withheld support for certain new policy recommendations at ICANN precisely because they "do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars and protecting the public from harms associated with bad actors seeking to exploit the domain name system."[5]

The fact of the matter is that if legitimate access seekers are more often than not denied the information necessary to prevent harms and protect the online ecosystem, then the very objectives of the revised NIS2 Directive will likewise come up short.

In order to achieve the shared objective of reliable and effective access to WHOIS information that will strengthen cybersecurity and protect against a litany of online harms, then the NIS2 Directive must confront the fragmented and failing system that empowers registrars and registries to respond to every request for non-public WHOIS data from legitimate access seekers and conduct a 'balancing test' where these entities alone weigh the legal, security, and enforcement interests of the access seekers against the privacy interests of the data subject. Responses to requests from legitimate access seekers are always inefficient and unpredictable, and more often than not insufficient, if there is any response at all.[6]

Further detail and justification for proposal: *Access to and disclosure of certain WHOIS data is in the public interest and it is also necessary for compliance with a legal obligation*

[4] ICANN Government Advisory Committee, "Minority Statement on the Final Report of Phase 2 of the EPDP on gTLD Registration Data," 24 August, 2020. Available at: https://gac.icann.org/statement/public/gac-minority-statement-epdp-phase2-24aug20.pdf

[5] See page 122 at https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtldregistration-data-2-31jul20-en.pdf Note that this document also contains similar concerns from four other parts of the ICANN multistakeholder community - the At-Large Advisory Committee, the Security and Stability Advisory Committee, the Business Constituency and the Intellectual Property Constituency.

[6] A recent audit from ICANN highlights related failures by registrars: https://www.icann.org/en/system/files/files/compliance-registrar-audit-report-2021-24aug21-en.pdf Of the 126 audited registrars (representing 90% of all g-TLD second-level domain names), 111 were found to have a deficiency that was "verified as noncompliance and requires an action from the Registrar to remediate the noncompliance," and 19 registrars "were unable to fully resolve their initial findings prior to the completion of the Remediation Phase" of the audit.

The current system for disclosure of WHOIS information stands in stark contrast to the NIS2 Directive and Article 23 in particular. However, the system is poised to persist unless the directive can provide greater clarity of intent when it comes to the duties of the processors of WHOIS data, so that all legitimate access seekers are provided accurate and timely critical data elements.

Article 23 proposes important reforms intended to remedy the situation; however, it is our view that the revisions and amendments considered at this stage still expose legal gaps to be exploited by cyber criminals and other bad actors. It is important for Article 23 to explicitly state that access to domain name registration data by legitimate access seekers serves the public interest and contributes to the security and stability of the Internet, providing the clarity needed for both requesters and controllers.

Therefore, we would propose a further amendment to Article 23, with the addition of a new subparagraph:

> (6) "Domain name registration data serves the public interest as provided for in Article 6(1)(e) of the GDPR; accordingly, Member States shall ensure that a natural person registrant's name, verified email address - and postal address, as appropriate to establish jurisdiction - are disclosed when requested by legitimate access seekers."

This proposal is designed to clarify and preserve the intent of the directive when it comes to domain registration data access. As the Commission stated in the initial report: "TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers."

We also see the opportunity for an additional amendment to Recital 69 that could likewise establish the processing of WHOIS data as a legal obligation, therefore relieving registrars and registries of balancing test duties under GDPR:

> (69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by essential and important entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services, **as well as access to domain name registration data by legitimate access seekers,** is necessary to comply with a legal obligation under this Directive and constitutes a legitimate interest of the data controller concerned, as referred to in point (c) paragraph 1, and point (f) paragraph 1 respectively of Article 6 of Regulation (EU) 2016/679.