Coalition for Online Accountability

Before the Bureau of Industry and Security
United States Department of Commerce
Washington, DC

15 CFR Part 7
[Docket No. 240119-0020] RIN 0694-AJ35

In re: Taking Additional Steps To Address the National Emergency
With Respect to Significant Malicious Cyber-Enabled Activities

April 29, 2024

The Coalition for Online Accountability[1] ("COA") appreciates the opportunity to respond to the Department of Commerce's notice of proposed rulemaking concerning "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities" ("NPRM").

COA is a longstanding group of companies, trade associations, and copyright member organizations dedicated to enhancing and strengthening online transparency and accountability by working to ensure that domain name and IP address WHOIS databases remain publicly accessible, accurate, and reliable, as key tools against online infringement of copyrights, as well as to combat trademark infringement, cybersquatting, phishing, and other illegal acts. There is no doubt that the motion picture, music, and video game industries have long suffered from widespread online piracy and other abuses. COA members are seeing deceitful use of their company logos, brands, and copyrighted works, such as: in bogus job postings used for phishing schemes; to sell pirated content, NFTs, or cryptocurrency; or to push vaping products (which could target underage users). Increasing the regulatory tools that should help to thwart such conduct and impersonations of governments and agencies is of great importance to COA's members. In these brief comments, we focus on the issues of most relevance and significance to our coalition and industries, and do not respond to every question in the NPRM. We thank the Department of

[1] While COA itself is a small organization, its members: Broadcast Music, Inc., the Entertainment Software Association, the Motion Picture Association, the Recording Industry Association of America, NBCUniversal Media, The Walt Disney Company and Warner Bros. Discovery, represent and/or employ hundreds of thousands of creators, whose copyrighted works and properties are made available legally online throughout the world and, unfortunately, are also subject to significant online piracy and counterfeiting.

Commerce for considering our input.

Our key comments to the NPRM, as further explained below, are as follows:

First, it is critical that U.S. domain name service providers be classified as U.S. Infrastructure as a Service (IaaS) providers for purposes of this rulemaking. The regulations requiring verification of the identity of foreign persons need to apply to persons or entities who make use of domain name related services offered by U.S. domain service providers. This is because malicious cyber-enabled activities are often launched from websites or emails that appear to originate from, or be associated with, legitimate domain names, and because bad actors often register these legitimate seeming domain names with malicious intent.

Domain name registrars are unarguably U.S. IaaS providers because they provide the ***means and instrumentalities for many malicious actors*** targeting key U.S. governmental authorities and major companies. The current carve out from the definition of IaaS providers for "domain name registration services for which a consumer registers a specific domain name with a third party, as that third party does not provide any processing, storage, network, or other fundamental computing resource to the consumer"[2] will create a loophole for these malicious actors.

Second, it is important that all U.S. domain name registries be required by the forthcoming regulations to maintain complete and accurate databases of the identity and contact information of all registrants for the domain names that such registries administer. For purposes of cybersecurity investigations, as well as the mitigation and prevention of cyberattacks and other malicious cyber-enabled activities, it is critical that government agencies (as well as cybersecurity investigators and organizations) be able to access this customer data directly from GoDaddy regarding the .US domain, and Verisign regarding any .com or .net domain name and other domain names that they administer.

THE NEXUS BETWEEN DOMAIN NAMES AND MALICIOUS CYBER-ENABLED ACTIVITIES

Domain name service providers play a crucial role in enabling malicious cyber activities by providing means and instrumentalities for many malicious actors. These malicious actors often seek to appear "official," by using .US domain names to impersonate U.S. governmental authorities and major companies, to defraud U.S. users and obtain sensitive data.

The new Interisle Consulting Group Report on the phishing landscape in 2023 reveals that domain names with the ".US" extension, representing the top-level domain for the United States, are prevalent in phishing scams. They are, in other words, a fundamental

[2] The Department of Commerce Notice of Proposed Rulemaking at 5702, https://www.federalregister.gov/d/2024-01580/p-47

resource for these scammers to perform as they do. The .US domain is notorious not only for the impersonation of the individuals and businesses but also the U.S. government, which itself is often targeted by phishing domains using this extension. Interisle's newest study examined six million phishing reports between May 1, 2022 and April 30, 2023, and found 30,000 .US phishing domains.[3] "Sadly, .US has been a cesspool of phishing activity for many years. As far back as 2018, Interisle found .US domains were the ***worst in the world*** for spam, botnet (attack infrastructure for DDOS etc.) and illicit or harmful content." (emphasis added).[4] Interisle reported that significant numbers of .US domains were also registered to attack some of the United States' most prominent companies, including Bank of America, Apple, Microsoft, Meta, Amazon, AT&T, Citi, Comcast, and Target.[5] "[A]t least 109 of the [analyzed] .US domains [] were used to attack the United States government, specifically the United States Postal Service and its customers."[6]

Even though .US domains are intended exclusively for U.S. citizens or individuals who can prove their physical presence within the United States, many foreign malicious actors have been able to easily circumvent that intention and have been able to use .US domains to target U.S. customers.

The National Telecommunications and Information Administration (NTIA), a branch of the U.S. Department of Commerce, oversees the .US domain. However, NTIA delegates the management of the .US domain to GoDaddy, the world's largest domain registrar. Despite NTIA regulations requiring verification of U.S. residency or organizational presence for .US domain registration, GoDaddy's management of this vetting process has been ineffective. Interisle's findings suggest that despite the "nexus" requirement intended to limit registrations to parties with a U.S. connection, the .US domain has a high number of phishing domains. All .US registrants must certify that they meet the NTIA's nexus requirements, however this "nexus requirement" "appears to be little more than an affirmative response that is already pre-selected for all new registrants" in the process of domain name registration with GoDaddy.[7]

This data supports the urgent need for the regulations being developed by the Department of Commerce in this rulemaking to apply ***unequivocally*** to U.S. domain name service providers, including all of the following: (i) domain name registries (such as Verisign and Public Interest Registry), (ii) domain registrars (such as GoDaddy and NameCheap),

---

[3] Why is .US Being Used to Phish So Many of Us?, KrebsonSecurity (September 1, 2023), https://krebsonsecurity.com/2023/09/why-is-us-being-used-to-phish-so-many-of-us/#:~:text=Domain%20names%20ending%20in%20%E2%80%9C [KrebsonSecurity].

[4] *Id.*

[5] Phishing Landscape 2023: An Annual Study of the Scope and Distribution of Phishing, InterIsle, at 20, (August 2023), https://static1.squarespace.com/static/63dbf2b9075aa2535887e365/t/65b966b32f82d97c583eccfc/1706649269929/PhishingLandscape2023.pdf.

[6] *Id.*

[7] See KrebsonSecurity, *supra* 2 for more detailed description of the registration and nexus verification process.

(iii) DNS providers (such as Cloudflare and OpenDNS), (iv) privacy/proxy service providers,[8] (v) domain name brokers, and (vi) domain name resellers. To this end, we advocate for the ***explicit inclusion*** of these service providers in the definition of U.S. IaaS providers.

As set forth in the NPRM, to deter foreign malicious cyber actors' use of U.S. IaaS products, and assist in the investigation of transactions involving foreign malicious cyber actors, E.O. 13984 requires more robust record-keeping practices and user identification and verification standards within the industry to better assist investigative efforts.[9] Given that malicious cyber actors—both foreign and domestic—make use of domains names to launch and conduct their cyberattacks and other online illegal activity, all of the domain name registration service providers enumerated in the preceding paragraph must be classified as U.S. IaaS service providers for purposes of this rulemaking in order for the regulations to have their intended impact of: (i) increasing transparency and accountability in the online environment, and (ii) decreasing malicious cyber activity. Like other U.S. IaaS service providers, domain name service providers must accurately identify their foreign customers (and arguably all of their customers) and verify their identity. Indeed, if domain name service providers actually engaged in rigorous identity verification, then malicious actors would be deterred from using their services.

To address effectively these security threats and to fulfill the goals established in E.O. 13984 and E.O. 14110, it is critical that the regulations developed and implemented by the Department of Commerce in this rulemaking apply broadly to providers of internet services, including domain name service providers.

"WHOIS DATA"— ITS RELEVANCE AND CURRENT STATUS

Currently, many domain name registrars turn a blind eye on the rampant domain name abuse practices. They provide the means and instrumentalities for impersonation making no effort to collect true and correct data about their clients.

On the effective date of the European Union's General Data Protection Regulation ("GDPR") and the Internet Corporation for Assigned Names and Numbers' ("ICANN") unilateral imposition of the Temporary Specification for gTLD Registration Data (the "Temp

[8] A privacy service lists alternative, reliable contact information, like an address or phone number, in WHOIS while keeping the domain name registered to its beneficial user as the registrant. A proxy service registers the domain name itself and licenses use of the domain name to its customer. The contact information of the service provider is displayed rather than the customer's contact information. The proxy service provider maintains all rights as a registrant (such as to manage, renew, transfer and delete the domain name), and assumes all responsibility for the domain name and its manner of use. See: https://whois.icann.org/en/privacy-and-proxy-services. In the case of both privacy service providers and proxy service providers, it is these providers that actually collect and possess the identity and contact information of the beneficial owner of the domain name.

[9] The Department of Commerce Notice of Proposed Rulemaking at 5699, https://www.federalregister.gov/d/2024-01580/p-3

Spec")[10] in 2018, ICANN expressed a commitment to "comply with the GDPR, while maintaining the existing WHOIS system to the greatest extent possible."[11] However, the WHOIS system has not been preserved to the greatest extent possible while still complying with the GDPR. On the contrary, there now exists a significant gap between the level of data access permitted under the GDPR and the real-world availability of WHOIS. In October 2018, the European Council stressed the negative consequences of enforcing the law online and to the rights of individuals caused by "the current situation where access to the non-public WHOIS data for public policy objectives is ***left at the discretion of registries and registrars*****,**" emphasizing the necessity to expedite the development of a unified access model.[12]

This situation with respect to lack of access to WHOIS data is due to registration data availability being severely limited by registrars and registries ("contracted parties"). Many contracted parties are ignoring or not fulfilling legitimate data requests or are imposing procedural or legal hurdles that make securing access impracticable. This is consistent neither with the commitment to preserve the pre-GDPR WHOIS system to the greatest extent possible, nor with the current contractual specification for contracted parties to provide "reasonable" access to legitimate data seekers. There is ***no justification for the redaction of data*** of legal person registrants or the overwhelming denial of reasonable access to personal WHOIS data for legitimate third-party interests, as permitted under the GDPR and as set forth in ICANN's own Temp Spec.

We are conscious of the concerns expressed by the commenters who ask the Department of Commerce to ensure that the processing of customers' data to carry out the provisions of any proposed regulation be consistent with the GDPR or CCPA and not frustrate ongoing negotiations to open the flow of data between foreign countries and the United States.[13] However, availability of domain name registration data cannot affect U.S. compliance with international obligations or affect the data transfers. To the contrary, the EU co-legislators have recognized the importance of accurate and accessible WHOIS data in the revised Network and Information Security Directive ("NIS2"). This Directive focuses on improving responses to significant cyber-enabled nefarious activity by permitting access to domain name registration data for investigations, mitigation, and enforcement. This data is collected and managed by registrars and, in most cases, registries as well.

The Department has an opportunity to further serve the public interest through

[10] Temporary Specification for gTLD Registration Data, https://www.icann.org/resources/pages/gtld-registration-data-specs-en/.
[11] *Id.*
[12] Item Note from General Secretariat of the Council Brussels to Permanent Representatives Committee dated 23 October 2018, https://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf (emphasis added).
[13] The Department of Commerce Notice of Proposed Rulemaking at 5700, https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious

WHOIS-related requirements such as those identified in Article 28 of NIS2, which include, *inter alia*:

- Domain name registries, registrars, and privacy and proxy providers must maintain complete, accurate, and verified registration contact data in a separate database.

- Where the information involves the data of legal persons, it must be publicly available, free of charge.

- Where the information involves the data of natural persons, the information must be disclosed upon request, to those with legitimate interest, such as to investigate, enforce and mitigate illegal activities, including malicious cyber-enabled activities.

Furthermore, the U.S. is a signatory to both the Budapest Cybercrime Convention and the Second Additional Protocol to the Budapest Convention.[14] The Second Additional Protocol to the Budapest Convention already recognizes the important role of domain name registrant data in confronting cybercrime. Article 6 of the Second Protocol addresses cross border requests for and access to domain registrant information "for identifying or contacting the registrant of a domain name." This information will be useful, however, only if the registration data delivered in response to such requests is accurate, verified, and consists of the data of the beneficial user of the domain name, not simply the data of a privacy or proxy service provider that may have been used in the domain name registration process.

Artificial restriction of WHOIS data availability has had a profoundly negative impact on the health of the domain name system ("DNS"). International law enforcement authorities, cybersecurity investigators, intellectual property rights holders and others are unnecessarily hindered in their ability to investigate and ultimately mitigate behavior that is damaging to the DNS ecosystem and Internet users broadly (and at a time of rapidly rising rates of DNS abuse in many key categories, such as phishing).

This all aids and abets bad actors seeking to use the DNS to impersonate governments, businesses, and other persons. There is very little disclosure occurring at all, even when disclosure requests, which impact a microscopic fraction of domain registrants who are reasonably identified as acting in bad faith, are reasonable, legitimate, timely, well-founded, supported by evidence, and the interests of the access seeker clearly outweigh privacy concerns of the data subject.

In fact, it is extremely difficult to retrieve non-public WHOIS data for any reason. Consider ICANN's letter[15] to U.S. Food and Drug Administration ("FDA") Commissioner

[14] https://www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat
[15] Letter of Robert M. Califf M.D., MACC Commissioner, U.S. Food and Drug Administration (June 14, 2022), https://www.icann.org/en/system/files/correspondence/marby-to-califf-14jun22-en.pdf

Robert Califf, which stated, in part:

> *It is not necessary to obtain a subpoena to gain access to non-public domain name registration data. Law enforcement and consumer protection agencies around the globe have relied on existing ICANN WHOIS policies to gain access to this data.*

The FDA's explanatory reply[16] was direct in stating that – in its experience – this is not factual. According to the FDA's letter:

> *Unfortunately…this is not the actual experience of FDA-OCI special agents who, when requesting non-public domain name registration data from any one of the over 2,400 ICANN-accredited registrars operating globally, are often asked to submit a subpoena, court order (sometimes within the jurisdiction of the registrar), or Mutual Legal Assistance Treaty (MLAT) to obtain such information.*

The FDA's experience comports with that of COA's members and other similarly situated parties. Indeed, despite statements by ICANN to the contrary, nearly every legitimate disclosure request submitted by or on behalf of COA's members has similarly and unnecessarily been met with demands for subpoenas or court orders or, worse, ignored outright.

Due to this unfortunate state of affairs, COA believes that the Department of Commerce's regulations should be expanded to specifically address unauthorized creation/use of Internet identifiers, such as gTLD and ccTLD (e.g., .US) domain names, apps, and block chain-based identifiers, to impersonate businesses and governments.

They should also include mitigation of "DNS Abuse"[17], the intentional registration and use of domain names for the purpose of impersonating, misleading or defrauding. Registrars and registries should be required to be responsive to abuse-related takedown requests that include credible evidence of abuse. The Rule should explicitly recognize as a "means and instrumentality" the failure to disclose non-public domain name registration data by a domain name registrar, registry operator, or privacy/proxy service provider upon receiving a credible request for such data in relation to impersonation being perpetrated through the relevant domain.

Should a cybersecurity problem arise with a .com or .net domain name, it makes no sense that government agencies need to track down one of 2,000 different registrars to try to obtain information about the identity of the person or organization that is the

[16] https://www.icann.org/en/system/files/correspondence/hermsen-to-marby-15jul22-en.pdf
[17] COA supports the approach to defining DNS Abuse taken in the EU's January 2022 *Study on Domain Name System (DNS) abuse*: https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f- 11ec-8c40-01aa75ed71a1.

registrant/owner of that particular domain name, especially since this information was already disclosed voluntarily to the registrar. Rather, U.S. government agencies should be able to go directly to the registry to obtain the relevant identity/WHOIS data. This will only happen, however, if the regulations issued by the Department of Commerce as part of this rulemaking require that service providers like Verisign and GoDaddy collect and maintain this full range of WHOIS data for both existing and newly registered domain names under all the top-level domains. There is no obstacle to complying with such an obligation other than a willingness to do so.

To enhance the cybersecurity of the United States and to assist in the fight against significant malicious cyber-enabled activities, it is important that all U.S. domain name registries be required to maintain complete and accurate databases of the identity and contact information of all registrants for the domain names that such registries administer.

RECOMMENDATION

We respectfully request the following revisions to the proposed Rule:

- The definition of a US IaaS should be supplemented with the following at the end thereof:

  > *The term also is inclusive of domain name service providers, such as domain name registrars, domain name registries, domain name privacy and proxy services, or other domain name authorities, regardless of whether they are accredited by an international multi-stakeholder policymaking organization.*

- The following suggested new section should be added in Subpart D in reference to §7.306, following (c) Public-private sector collaboration:

  (d) Specific Requirements for domain name service providers.

  1. A domain name registrar, registry, privacy service, proxy service, or other domain name registration authority must have accurate and complete domain name registration data in its registration directory service for each domain name that it sponsors, sells, or maintains as part of the relevant registry, including the domain name registration data of the privacy or proxy customer, and must act expeditiously to correct any inaccurate domain name registration data found through its own due diligence or after notification from another party.

  2. The domain name registrar, registry, privacy service or proxy service, or other domain name authority must make publicly available through its registration directory service, including on its website, in a location accessible to the public

free-of-charge, at a minimum, all domain name registration data of legal persons as identified in subsection (9).

3. For any domain name registration data not publicly available under subsection (2), the domain name registrar, registry, privacy service, proxy service or other registration directory service maintained by a domain name registration authority must disclose the requested domain name registration data (as identified in subsection (9)) within 72 hours after receipt of a good faith disclosure request reasonably claiming violations of this Section or of law or citing other legitimate purposes for accessing the personal data. The domain name registrar, registry, privacy service, proxy service, or other Registration Directory Service maintained by a domain name registration authority shall disclose such contact data free-of-charge to the requestor. Such disclosed data must consist of the data of the registrant of record and the domain name registration data of the privacy or proxy customer, if applicable.

4. The domain name registrar, registry, privacy service, proxy service, or other domain name registration authority must disable, disrupt, or suspend any domain names used for domain name abuse within 48 hours of receipt of a notice submitted in good faith from a Trusted Notifier.

5. The domain name registrar, registry, privacy service, proxy service, or other domain name registration authority must provide to the Trusted Notifier, upon request and within 48 hours of receipt of notice, a list of all other domain names under its authority or services that share the same domain name registration data as the specific domain name identified by the Trusted Notifier as being used for domain name abuse.

6. In the event there is a reasonable basis to determine that any of the domain names identified in the list under subsection (5) are likely to be used for domain name abuse, such domain names shall also be disrupted, disabled or suspended by the domain name registrar, registry, privacy service proxy service, or other domain name registration authority within 48 hours of the disclosure of the list.

7. “Domain name” means a unique string that forms the basis of the uniform resource locators (URLs) consisting of a generic top-level domain name, country code top-level domain name, or an alternative root or blockchain domain name.

8. “Domain name abuse” means any activity that makes, or intends to make, use of domain names, the domain name system protocol, or any digital identifiers that are similar in form or function to domain names to carry out deceptive, malicious, or illegal activity.

9. “Registration directory service” (commonly referred to as WHOIS) means the complete and accurate database, maintained by a domain name registry and/or registrar for each domain name registered or sponsored by it, containing information necessary to identify and contact the holders of the domain names, and the points of contact administering each domain name. This database shall include, but is not limited to, information for each domain name in the domain name registry, the registrant’s name, address, telephone number, contact email, and the points of contact for the administrator of the domain name, if it is different from that used by the registrant. It shall also include the name, address, telephone number, and contact email for any reseller or any privacy or proxy customer.

10. “Free of charge” means that no fees may be charged or other consideration required for access or disclosure of information in the WHOIS or similar database, and no additional terms and conditions may be imposed on such access or disclosure by the registry, registrar, proxy provider, privacy provider, reseller or other entity authorized by a registration authority to provide access to or disclosure of the contact information maintained in the domain name registration directory, unless such additional terms and conditions are required by applicable law.

11. “Privacy service” means a service that allows a customer to register a domain name as the registered domain name holder, in which the customer's name appears unredacted in the “registrant name” field in the publicly available Registration Directory Service, and includes publication of alternative contact information (in place of the customer's personal contact information).

12. “Proxy service” refers to a service that allows a customer to use a domain name without displaying any of the customer's information in a Registration Directory Service. The proxy service provider is the registrant of record and the registered domain name holder and provides alternative contact information for the privacy or proxy customer.

13. “Trusted Notifier” means an (i) organization, business, or government agency that (i) has been vetted under processes to be developed by the Department of Commerce and is likely to be the target of significant malicious cyber enabled attacks, or (ii) cybersecurity professionals or organizations that engage in detection, mitigation, and prevention of significant malicious cyber enabled attacks.

We again thank the Department of Commerce for considering our comments.

Respectfully submitted,

J. Matthew Williams
Mitchell Silberberg & Knupp LLP

1818 N Street, NW, 7th Floor
Washington, DC 20036
Email: mxw@msk.com; Tel: 202-355-7900
Executive Director and Legal Counsel to COA

Eleanor M. Lackman
Mitchell Silberberg & Knupp LLP
437 Madison Avenue, 25th Floor
New York, NY 10022-7001
Email: eml@msk.com; Tel: 212 509-3900
Legal Counsel to COA