National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4701
Attn: Susan Chalmers
Washington, DC 20230

May 31, 2023

Re: Docket ID NTIA–2023–0006

On behalf of the Coalition for a Secure & Transparent Internet (CSTI), we offer the following comments in response to the National Telecommunications and Information Administration (NTIA) Request for Comments, regarding the .US WHOIS.

CSTI is a group of stakeholders who share concerns about losing access to domain name registration information for general top-level domain names (gTLDs), referred to as "WHOIS." WHOIS information identifies the individuals or organizations behind a domain name registration or website. This information was publicly available until the overly broad interpretation of the European Union's General Data Protection Regulation (GDPR) was implemented in 2018 by the Internet Corporation for Assigned Name and Numbers (ICANN), and the ICANN contracted parties like GoDaddy that manage the .US domain name service. Since then, it has become increasingly difficult, if not impossible, for regular Internet consumers, law enforcement, cyber security investigators, consumer protection agencies, and brand owners to confirm the identities of those on the other side of the screen.[i] Having access to domain name registration information is vital in the online world to verify the true identity of an entity and prevent impersonation. This problem is even more critical during crises like the COVID pandemic or a cyber attack. Furthermore, the lack of access to WHOIS information hinders both consumers and government agencies from effectively pursuing legal action, such as obtaining restraining orders, to safeguard individuals and organizations from deceptive websites.

CSTI would encourage NTIA to consider the potential impacts of this proposal on issues related to cybersecurity, fraud and consumer/child protection when proposing such drastic changes to the .US space. The failure of NTIA to provide any information or questions in its request for comments regarding the risks to cybersecurity and consumer/child protection posed by their proposal, which would create a “dark WHOIS,” is highly disappointing.

The following is a collection of some of the experiences we have witnessed as a direct result of ICANN and the contracted parties overreaction to the EU’s implementation of the GDPR. Also informative is how countries like Denmark have responded and the steps being undertaken currently within the EU. Application of similar policies to the .US could be *additionally*

detrimental given the expectations consumers have around visiting websites that have .US associated with them.

At CSTI, we believe that the current .US WHOIS system is functioning adequately to provide cybersecurity experts, child safety groups, law enforcement, consumer protection agencies, and IP holders access to necessary and critical registrant data to protect against the misuse of .US domain names that put U.S cyber security and consumer protection at risk. We also believe the .US Annual WHOIS Accuracy Reports, which are specifically required in the .US contractor contract, should be made accessible to the public. This will improve transparency and allow individuals to better understand the cybersecurity and consumer protection risks associated with the .US domain name system. Providing this information will also enable interested parties to conduct a comprehensive analysis and determine if any further adjustments are necessary for accessing accurate .US WHOIS information. Various federal agencies have emphasized that the unavailability of WHOIS information has had serious implications for national security and consumer protection.

In 2020, Congressman Latta (R-OH) wrote to several federal agencies about the impact the loss of access to WHOIS information has had on combating fraud and protecting consumers. In response to that inquiry, the Federal Trade Commission (FTC) noted that:

> "Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud. **The FTC uses this information to help identify wrongdoers and their locations, halt their conduct and preserve money to return to defrauded victims**."[ii] (emphasis added)

Clearly, the connection between fraud and domain name registration information has enormous ramifications for not only identifying that an impersonation is taking place but also ensuring that remedies can be pursued for the injured party.

The Department of Homeland Security's Homeland Security Investigations (HSI) responded similarly to an identical inquiry from Rep. Latta (R-OH), noting:

> "HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. **If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain."**[iii] (emphasis added)

In its response, HSI raises a critical point to stopping these fraudulent activities (including impersonation), and that is the need to identify all domain name registrations that are used in the perpetration of a criminal activity. Consider the study conducted by Interisle Consulting Group ("*Criminal Abuse of Domain Names: Bulk Registration and Contact Information Access*") which found that "cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domain names for their attacks.[iv] Domain name registration information, and the databases that contain that information, enable that level of analysis and give us the ability to understand how these networks are connected and deny their access before harm occurs."

The FTC has also been vocal on the role domain name registration plays in combatting fraudulent activity and, specifically, in empowering consumers to protect themselves. In its response to Rep. Latta, the FTC noted how the loss of access to this information, broadly, has limited the resources consumers could use to verify who is on the other side of the screen:

> "This lack of access also limits consumers' ability to identify bad actors using WHOIS information. **Prior to the GDPR, thousands of the complaints filed in our Sentinel compliant database referred to the filer's use of WHOIS data to identify businesses involved in spyware, malware, imposter scams, tech support scams, counterfeit checks, and other malicious conduct.**"[v] (emphasis added)

These complaints served as "force multipliers" for enforcement agencies as they initiated many investigations into fraudulent activity.

The U.S. Food & Drug Administration also weighed in on its use of domain name registration information and its role in combating fraud:

> "Greater WHOIS access would significantly assist FDA with the identification of individuals and firms illegally selling FDA-regulated products online. **WHOIS adds a layer of transparency to website, online marketplaces and vendors, and enables our regulatory cybersecurity and law enforcement personnel to link seemingly disparate websites into organized affiliated networks and track historical domain name ownership**." (emphasis added)

U.S. policy clearly states that free, accurate, and accessible WHOIS data is in the public interest. The Federal Bureau of Investigation (FBI) and the FTC have emphasized the significance of accessing accurate WHOIS information in recent presentations to ICANN's Governmental Advisory Committee (GAC), thus reaffirming the U.S.'s stance.[vi] [vii] This policy is also reinforced by federal laws such as the CAN-SPAM Act (P.L. 108-187) and the Anti-cybersquatting Consumer Protection Act (P.L. 106-113). The CAN-SPAM Act requires that for any commercial message, "the originating domain name and email address – **must be accurate** (emphasis added) and identify the person or business who initiated the message."[viii] This requirement is a vital first step for consumers to verify the identity of the individual with whom they are engaged. The

Anti-cybersquatting Consumer Protection Act prohibits the use of 'identical or confusingly similar' marks or other intellectual property for profit. Recognizing the ease with which someone can impersonate another online, the Anti-cybersquatting Consumer Protection Act also includes that prohibition to include domain names.[ix]

CSTI appreciates the opportunity to comment on the underlying question and stands ready to work with NTIA to address concerns that underlie the NTIA's Request for Comments, regarding the .US WHOIS. But the U.S government must ensure that any changes to the ability to access .US WHOIS information will not interfere with effectively and efficiently helping to verify the identities of those attempting to impersonate another entity through a .US domain name. Online scams, such as malware, ransomware, phishing, and cyber-attacks, all have one thing in common: a registered domain name. To protect consumers and children from such threats and ensure cybersecurity, it's essential to prevent any actions that weaken or obstruct access to .US WHOIS information.

For example, Denmark has determined that the public interest in accessible WHOIS data for its .dk country-code top-level domain ("ccTLD") is significant enough to make such information available to the public, even when a registrant is a natural person. To that end, Denmark has enacted legislation requiring that the name, postal address, and phone number of all .dk registrants, with narrow exceptions, be publicly accessible. Denmark has expressed to ICANN that their goal in implementing this provision is to **create a domain with excellent transparency while balancing privacy interests with other factors**. **The provision aims to increase accountability among registrants, thereby reducing the prevalence of illegal websites and online harassment.** (emphasis added)

Furthermore, the NIS2 Directive of the European Parliament and Council, aimed at ensuring a high level of cybersecurity and consumer protection throughout the European Union, has recently been implemented and states, "[M]aintaining accurate and complete databases of domain name registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union. For that specific purpose, TLD name registries and entities providing domain name registration services should be required to process certain data necessary to achieve that purpose." The NIS2 further states "[T]he availability and timely accessibility of domain name registration data to legitimate access seekers is **essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents**." [x] (emphasis added)

Given the results we have seen from cybersecurity analysts and our own federal agencies in the wake of the implementation of the EU's GDPR, given what we have seen from Denmark's own experience in managing its ccTLD and the resulting data and given what the European Union is doing to re-establish an appropriate balance with respect to domain registration information, CSTI recommends NTIA collaborate with Congress to pass legislation that guarantees high-

volume and individual access to accurate .US domain name registrant information for legitimate purposes in a timely fashion.

Access to this data is crucial for federal, state, and local government law enforcement and consumer protection agencies, and businesses to respond effectively and efficiently to criminal activities such as cyber-attacks, fraud, and false impersonation. Given NTIA's role on the GAC, which advises the ICANN board, NTIA must ensure that legitimate access to accurate .US WHOIS is the "Gold Standard."

CSTI would be please to answer any questions or provide further information on its views. Thank you for the opportunity to comment.

Sincerely,

The Coalition for a Secure & Transparent Internet (CSTI)

---

[i] https://apwg.org/m3aawg_apwg_whois_user_survey_report_2021/
[ii] https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
[iii] https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
[iv] https://www.interisle.net/criminaldomainabuse.html
[v] https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
[vi] https://see2do.info/ICANN75PublicSafety
[vii] https://see2do.info/icann73GACDNSPresentation
[viii] CAN-SPAM Act: A Compliance Guide for Business | Federal Trade Commission (ftc.gov)
[ix] https://www.govinfo.gov/content/pkg/PLAW-106publ113/pdf/PLAW-106publ113.pdf
[x] https://www.nis-2-directive.com/