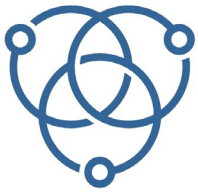

COALITION FOR ONLINE ACCOUNTABILITY
COA

The Honorable Arielle Roth

Assistant Secretary of Commerce for Communications and Information

Administrator, National Telecommunications and Information Administration

U.S. Department of Commerce

1401 Constitution Avenue, N.W.

Washington, DC 20230

cc: The Honorable Howard Lutnick

Secretary of Commerce

March 20, 2026

Dear Assistant Secretary Roth,

The Coalition for Online Accountability ("COA") consists of six leading copyright industry companies, trade associations, and member organizations of copyright owners. COA seeks to improve the practices of online service providers, with a particular focus on domain name service providers, to strengthen safety and accountability in the online environment and to combat illegal online activity. COA chose not to submit our concerns in response to the recent Request for Proposal (RFP) regarding the administration of the .us country-code top-level domain (.us ccTLD). Instead, we are expressing our concerns directly to NTIA and the Department of Commerce regarding the effective and safe management of the global domain name system (DNS), and in particular the .us ccTLD. The U.S. government has full discretion and authority to set policies and requirements for its own .us ccTLD to ensure its safety and legitimacy. Therefore, the purpose of this letter is

to provide NTIA with information in order to set the important and appropriate policies and processes that should be required to be implemented by any potential administrator of the .us ccTLD.

We write to express our serious concern about the persistently high and disproportionate levels of DNS abuse in the .us country-code top-level domain and the failure to implement widely recognized best practices that could significantly reduce such abuse. The ccTLD that represents the United States, .us, is closely associated in the public mind with the U.S. government and the American people and therefore should be among the most trusted and best-protected namespaces on the internet. Unfortunately, this is not the case. Instead, the .us ccTLD features elevated rates of phishing, malware distribution, and other cybercrime, particularly when compared to the ccTLDs of European countries.

Multiple studies and expert reports, including those issued by M3AAWG and Brian Krebs' "Why is .US Being Used to Phish So Many of Us?" have documented the alarmingly high rates of abuse and cybercrime that persist on the .us ccTLD. Indeed, the Cybercrime Information Center reported that the .us ccTLD had the 5th highest number of cybercrime domains of any ccTLD for the period of September 2023 to August 2024. What makes this even more disturbing is that compared to several other ccTLDs, the U.S. has a relatively small number of registered domain names. For example, Germany had over 17 million domain names registered in its .de ccTLD as of August 2024, with 28,846 identified as associated with cybercrime. As of the same time period, the United States had under 2.1 million domain names registered in its .us ccTLD, with 47,953 identified as associated with cybercrime. (Cybercrime Activity in Top-level Domains (TLDs) September 1, 2023 - August 31, 2024 — Cybercrime Information Center) . These figures and the levels of criminal activity and abuse that they represent should be unacceptable to both the U.S. government and the U.S. public.

European ccTLDs demonstrate that robust collection, verification, and accessibility of accurate domain name registrant (WHOIS) data, combined with proactive and reactive safeguards, can dramatically lower cybercrime and abuse rates, even where the underlying market share of domains is significant. Yet in .us, many of these proven safeguards have not been systematically adopted, despite clear, concrete proposals that have been presented to U.S. authorities and the .us operator.

In October 2023, COA and allied experts submitted a set of "Recommended Practices to Reduce the Level of Abuse on .us ccTLD "outlining pragmatic measures that the registry could implement without burdening legitimate users. These recommendations include, among others: prohibiting bulk registrations, especially via domain-generation algorithms;

implementing effective "know your customer" verification of registrants; requiring proof of compliance with the .us nexus requirement; employing predictive abuse-detection tools and trusted third-party data feeds; maintaining a refreshed, publicly accessible WHOIS database for .us, and establishing trusted notifier arrangements with government agencies and qualified non-governmental organizations. These steps align closely with the best practices recognized in the European Commission's study on DNS abuse and in the EU's NIS2 Directive Article 28, both of which emphasize accurate, verified registration data and timely access for legitimate investigators as central to preventing and mitigating DNS abuse and cybercrime.

Despite the availability of these concrete processes and policies, .us remains poorly managed, with high levels of abuse and cybercrime that are inconsistent with its status as the United States' own country-code domain. The continued absence of strong verification of registrant data, restrictions on bulk registrations, and systematic use of predictive abuse-detection tools effectively allows bad actors to leverage .us as a launchpad for cybercrime. This not only harms U.S. consumers and businesses but also undermines public trust in a namespace that should symbolize authenticity and accountability.

COA members are particularly troubled by the gap between what leading ccTLDs have demonstrated is possible and what is currently being done for .us. European ccTLDs, for example, have shown that when registries and registrars verify WHOIS data, prohibit or tightly constrain bulk registrations, and respond quickly and at scale to abuse reports, abuse rates fall sharply even as overall registration volumes remain robust. Similarly, the NIS2 Article 28 implementation work highlights the importance of: (1) verified, accurate registrant data; (2) independent, registry-level databases (thick WHOIS); (3) timely, confidential access for law enforcement and other legitimate access seekers; and (4) meaningful consequences, including suspension, for domains registered with materially false or incomplete data or malicious intent. These principles are equally applicable to .us and, in our view, should inform U.S. policy for its national ccTLD.

In addition, the experience of law enforcement and cybersecurity investigators shows that delayed or incomplete access to registrant data, reliance on privacy/proxy services to shield underlying beneficial users, and the lack of reverse-WHOIS capabilities significantly impede efforts to prevent and respond to cybercrime as stated by M3AAWG and the Anti-Phishing Working Group (APWG) in their joint recommendations to ICANN in November 2021.

When criminals can anonymously register large numbers of .us domains with minimal verification and little risk of prompt suspension, they are effectively given a powerful tool for victimizing U.S. residents, small businesses, and critical institutions. Such an outcome

is fundamentally at odds with the public-interest obligations that should attach to the administration of the United States' own country-code domain.

We therefore respectfully urge the Department of Commerce, acting through NTIA and in coordination with other relevant agencies, to:

1. Directly engage with the .us registry operator to ensure adoption of the recommended practices COA and others have articulated, including robust know your customer-style verification of registrants, prohibition of bulk registrations using algorithms, predictive abuse-detection and early-warning systems, and maintenance of accurate, accessible WHOIS data for .us.

2. Require the registry to implement clear, enforceable policies that mandate freezing and, where appropriate, suspension of .us domains registered with materially false or incomplete data, or identified as maliciously registered, as well as reverse-WHOIS checks to identify and address clusters of abusive domains registered with the same data.

3. Establish or formalize trusted notifier and trusted flagger arrangements between the .us registry and U.S. federal and state law enforcement agencies, relevant regulators, and vetted non-governmental organizations specializing in cybersecurity, child protection, medicine and patient safety, and intellectual-property enforcement, coupled with prompt action on substantiated abuse notices.

4. Promote policy alignment between U.S. practice for .us and the emerging international standards reflected in NIS2 Article 28 and the European Commission's recommendations on DNS abuse, so that the national ccTLD of the United States reflects best-in-class safeguards rather than lagging far behind peer jurisdictions concerning the safety of their ccTLDs.

We recognize that NTIA has already highlighted the importance of DNS health and abuse mitigation in its oversight of other major registries and in its engagement on international cybercrime and cybersecurity frameworks. In our view, the same level of urgency and rigor should now be applied to .us, given its national significance and the heightened expectations of trust that the American public naturally attaches to domain names ending in .us. Strengthening .us against DNS abuse and cybercrime would not only reduce concrete harms, but would also signal that the United States is prepared to lead by example in aligning its own domain-name infrastructure with the highest standards of accountability and safety.

COA and its members stand ready to assist NTIA and the Department of Commerce in this effort. We would welcome the opportunity to participate in any consultations, workshops, or multi-stakeholder processes you may convene to examine .us abuse issues in greater detail and to help design and implement practical solutions.

Thank you for your consideration of our concerns and for your continued leadership on issues critical to the security and trustworthiness of the DNS.

Respectfully submitted,

David Hughes

Executive Director

Coalition for Online Accountability (COA)

7701 Westfield Drive, Bethesda, MD, 20817

https://onlineaccountability.net/

David@davidhughes.ca

m: 917-733-4494