

2024-10-31

Subject: .COM Opposition - Internet Gatekeeper's Threat to U.S. Business and National Security Integrity 

cc:

Senator Richard Blumenthal, Senator Chris Murphy, Attorney General Merrick B. Garland, U.S. Department of Justice, Secretary Alejandro Mayorkas, Department of Homeland Security, Joseph V. Cuffari, Inspector General, Department of Homeland Security, Shalanda D. Young, Director, Office of Management and Budget (OMB), President Joe Biden, Vice President Kamala Harris

Dear Stakeholders:

We are writing to express serious concerns regarding the management of Critical Information Infrastructure (CII), specifically the Internet's Domain Name System (DNS), the Top-Level Domain (TLD) .COM, and the Internet's Root Zone file, which includes all TLDs such as .NET and .ORG. Verisign's dual role as the operator of .COM and the Root Zone Maintainer, along with former Government Contractor ICANN, positions them as dominant gatekeepers within the global DNS ecosystem, controlling CII that underpins both the Internet and the global digital marketplace. The placement of .eco into the marketplace is particularly concerning, as findings revealed that the Department of Commerce (DoC)/National Telecommunications and Information Administration (NTIA), as part of the Root Zone Management (RZM) Partnership, failed to prevent non-compliant and potentially unlawful actions that **usurped U.S. laws, agreements, and contracts** under **Cooperative Agreement #9218724**, thereby compromising compliance, national security, fair competition, and the integrity of the U.S. digital marketplace.

This illustrates the RZM Partnership's non-compliance and monopolistic power to unilaterally determine which Registry Operators (ROs) can pass through its exclusive gateway to access the marketplace—a gateway over which Verisign holds complete control. Such actions are deeply troubling, especially in light of the federal oversight requirements under U.S. Cooperative Agreement #9218724, which mandates that Verisign ensure all root zone changes receive proper federal authorization from the (DoC)/ (NTIA) to safeguard the integrity and security of the Internet DNS.

By proceeding with the <.eco> delegation, the RZM Partnership exercised unbridled discretion, usurping the Agreement, contracts, rules, and laws while performing arbitrary "gateway" services. The partnership failed to adhere to the performance requirements of Cooperative Agreement #9218724, breaching its obligations and compromising the security and stability of the Internet DNS. This action facilitated the insertion of .eco into the marketplace on behalf of a conflicted foreign company. Such actions expose vulnerabilities that jeopardize U.S. innovation, market access, and competitive fairness, ultimately undermining American interests.

The Threat to American Innovation and Security

Verisign's role as the exclusive RZM and .COM operator has serious implications for American innovation, market integrity, and national security. Its unchecked influence over DNS operations has opened the door to foreign manipulation of the DNS ecosystem, eroding the principles of fair competition and intellectual property protection that underpin U.S. leadership in global innovation and security.

Background: .ECO®'s Market Access Blocked in Favor of Foreign Interests

planet .ECO® LLC (.ECO®), a fully compliant applicant in the 2012 New gTLD Program, met all necessary legal, regulatory, and contractual requirements to enter the marketplace and provide .ECO® top-level domain (TLD) services. Despite adhering to these stringent standards, its legitimate entry was systematically obstructed. Unauthorized and/or illegal changes to the Internet's root zone led to the transfer of control over its intellectual property to conflicted foreign entities, who continue to operate the .eco TLD outside the boundaries of U.S. law. These noncompliant actions usurped constitutional protections related to property rights and fair competition, directly contravening Verisign's obligations under the Cooperative Agreement. Such failures not only violate commitments to U.S. businesses but also erode principles of fair market access, threatening the integrity of American innovation and the rule of law.

Broader Implications for All U.S. Businesses

This issue extends far beyond .ECO® and impacts on the broader marketplace. The risks posed by Verisign's actions—including monopolistic control, gatekeeping and conflicted foreign interference—threaten every American business. Without intervention, all U.S. companies remain vulnerable to the same risks: restricted market access, loss of IP protections, and exposure to manipulation by conflicted foreign entities. Such outcomes directly undermine U.S. innovation, market leadership, and security.

Reasons for Opposing Verisign's Renewal as .COM RO

1. Risk to National Security and CII

Given the critical role of .COM in U.S. and global e-commerce, Verisign's management of this infrastructure must align with the highest standards of compliance and oversight. However, Verisign's unauthorized delegation of <.eco>—without NTIA's required approval—demonstrates a breach of Cooperative Agreement #9218724, under which Verisign is obligated to ensure all root zone changes are properly authorized. This failure in compliance directly impacts Verisign's role as the .COM Registry Operator, as *the same agreement governs its management of both .COM and the Root Zone*. Allowing Verisign to continue in this dual role without accountability for prior breaches risks reinforcing non-compliance, potentially compromising the security and integrity of the DNS and jeopardizing U.S. national security interests.

2. Compliance Failures in DNS Management

The .ECO® case serves as a critical example of Verisign's failure to comply with explicit federal oversight requirements, under the Agreement. Verisign's unilateral root zone changes or allowance, bypassing requisite U.S. Department of Commerce / NTIA authorization¹, violate the Agreement, authorization approval, which

¹ https://www.ntia.gov/sites/default/files/publications/ntias_role_root_zone_management_12162014_0.pdf

mandates federal supervision to protect CII. This disregard for mandated oversight jeopardizes the security and stability of the .COM domain and erodes the integrity of the DNS infrastructure as a whole.

3. **Conflict of Interest, Gatekeeping and Monopoly Control**

Verisign's dual role as the exclusive .COM Registry Operator (RO) and a RZM represents an inherent conflict of interest. This dual position enables Verisign to shape DNS access and market entry, often to its commercial advantage. The exclusion of planet .ECO® LLC from the <.eco> TLD delegation illustrates this conflict, where Verisign's gatekeeping was used in the denial of market access for a compliant U.S.-based competitor with legitimate trademark rights. Renewing Verisign's contract would reinforce its monopolistic control, limiting competition and stifling innovation. This issue extends beyond .ECO® and poses significant risks to the broader marketplace. Without intervention, all U.S. companies face the same vulnerabilities: restricted market access, diminished intellectual property protections, and potential manipulation by conflicted foreign entities, as demonstrated in the .ECO® case.

4. **Failure to Uphold U.S. Trademark and Small Business Protections**

Verisign has failed to uphold protections for U.S.-based trademark holders and small businesses. The unauthorized delegation of <.eco> to a conflicted foreign entity contradicts U.S. trademark protections and the principles in **President Clinton's Framework for Global Electronic Commerce**, which emphasized fair competition and IP protection. Given the significance of .COM to U.S. and global e-commerce, appointing a new RO committed to compliance and respect for U.S. law is essential to safeguard American innovation and ensure a fair marketplace.

Conclusion

The actions of two private corporations, **Verisign and ICANN**, alongside the U.S. Department of Commerce's oversight, demonstrate a troubling exercise of unbridled power, effectively **usurping U.S. laws, rules, regulations, agreements, and contracts** designed to protect Critical Information Infrastructure (CII). The Department of Commerce, overseeing the NTIA and United States Patent and Trademark Office (USPTO), plays a critical role in ensuring compliance and protecting U.S. interests. However, the breaches associated with the <.eco> delegation highlight a significant failure, creating risks of non-compliance, conflicts of interest, and potential threats to U.S. national security and market integrity. Renewing Verisign's role as the .COM Registry Operator would reinforce these vulnerabilities and undermine the principles of fair competition and IP protection outlined in President Clinton's **Framework for Global Electronic Commerce**. To uphold the foundational values of U.S. innovation and secure the DNS as CII, we urge the rejection of Verisign's renewal, and the appointment of a successor Registry Operator RO committed to transparency, compliance, and safeguarding U.S. interests.

Call to Action: Ensuring American Security and Innovation

We respectfully call upon U.S. oversight authorities, including the U.S. Department of Commerce, to address the failures by Verisign, ICANN, and the DoC/NTIA in complying with Cooperative Agreement #9218724, Contract SA1301-12-CN-0035, and relevant cybersecurity and Internet governance laws compromised during



the unauthorized delegation of <.eco>. The **.ECO® case** illustrates how a lack of comprehensive oversight and enforcement allows private entities to usurp the **Constitution** and the authority of the **U.S. Department of Commerce**, undermining U.S. laws and agreements designed to protect due process, commerce, and property rights. This overreach threatens the safety, security, and integrity of the Internet and poses serious risks to **American innovation, fair competition, and intellectual property protections**—elements vital to U.S. business and national security.

To align with the framework’s vision of a fair and secure digital marketplace, we request that the **rights to the .ECO® trademark** be fully restored to planet .ECO® LLC for rightful utilization as a gTLD in the marketplace. This moment is an opportunity for the **U.S. government** to reinforce the integrity of America’s core Internet infrastructure by appointing a Registry Operator RO that prioritizes DNS security, compliance, and an equitable marketplace for U.S.-based companies.

Thank you for addressing these critical issues and for prioritizing the **security, fairness, and competitiveness** of the American Internet landscape.

Respectfully,

Jean D. William, CEO
planet .ECO® LLC & .ECO® LLC
dba – **.ECO® Made in America**

cc:

Ms. Jen Easterly
Director
Cybersecurity and Infrastructure
Security Agency Stop 0380
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380 -
jeneasterly@cisa.dhs.gov
Central@Cisa.dhs.gov

Attorney General Merrick B. Garland
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
Department of Homeland Security
2707 Martin Luther King Jr Ave SE
Washington, DC 20528-

Office of the Inspector General, Department of
Homeland Security
Joseph V. Cuffari, Inspector General
Office of Inspector General
Department of Homeland Security
245 Murray Drive, SW, Building 410
Washington, DC 20528-0305

Mr. Helder Agostinho
Deputy Assistant Director, Technology
Enforcement Division
Federal Trade Commission
hagostinho@ftc.gov

President Joe Biden
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Vice President Kamala Harris
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Office of Management and Budget (OMB)
Shalanda D. Young, Director
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Senator Richard Blumenthal
90 State House Square, 10th Floor
Hartford, CT 06103
collin_anderson@blumenthal.senate.gov
Attn: Mr. Collin Anderson

Senator Chris Murphy
Colt Gateway
120 Huyshope Avenue, Suite 401
Hartford, CT 06106
Email: casework_murphy@murphy.senate.gov
Attn: Kylee Dostie

