An Open Letter to United States Policymakers

Re: i2Coalition Expands VPN Trust Initiative - Announces Principles to Evaluate VPN Security Technologies

On behalf of the Internet Infrastructure Coalition's (i2Coalition) [VPN Trust Initiative](#), I am writing to announce the launch of its [core principles](#) for Secure VPN Technologies (Virtual Private Networks). This initiative is especially critical given the need for secure communications during times of local and global crises, such as we're experiencing today in the Russian invasion of Ukraine.

The mission of the industry-led VPN Trust Initiative is to establish model principles and practices, to guide the VPN industry as it supports millions of users across the world.

VPNs provide a secure and protected network connection when someone is using a public network. They deliver enhanced security and privacy, ease of collaboration, and Internet performance, while reducing geographic restrictions, and ensuring safer data transfers.

Since Russia began its brutal assault on Ukraine, including a devastating cyber war, both Ukrainians and Russians have turned to VPNs in growing numbers to obtain private and secure access to truthful information. They have also made the switch to VPNs in order to more readily communicate with friends and loved ones without fear of repercussions.

Beyond areas in conflict, experts estimate that 30 percent of Internet users have utilized a VPN or proxy server in the past month, and the global VPN market is predicted to increase by [$34 billion](#) from 2021 to 2026. In response to this surge in VPN use for secure communications, the VPN Trust Initiative Principles were developed from a collaboration of industry, civil society, and outside experts. The principles offer public and transparent guidelines for industry self-regulation. They focus on five key areas: security, privacy, advertising practices, disclosure and transparency, and social responsibility.

- <u>Security</u> – VPNs will use the necessary security measures including strong encryption and authentication protocols to appropriately address risks.
- <u>Privacy</u> – VPNs should keep as little data as they deem necessary to provide the service, and only produce data to law enforcement when legally required.
- <u>Advertising Practices</u> – Given the complexity and different use cases for VPNs, claims must not mislead.
- <u>Disclosure and Transparency</u> – To drive trust, member companies must take steps towards informing users and the public about their actions and procedures.
- <u>Social Responsibility</u> – VPNs will continue to provide greater security and privacy - social goods that are important to those trying to make the world a better place.

We hope that by sharing these principles with policymakers, we can establish a beneficial accountability model that builds strong trust and security, drives greater adoption, and helps VPN technologies thrive.

We will continue to evaluate these voluntary standards and update them as needed.
VPNs are a crucial and growing part of our digital world, so guiding the development of best practices for this technology is a key part of the i2Coalition's commitment to protect innovation and encourage industry growth — an essential part of the global economy.

For more information, please see [the complete description of the VPN Trust Principles](#).

If you have questions about the VPN Trust Initiative, please contact Elisabeth Klughardt, Chief of Staff for i2Coalition at elisabeth@i2coalition.com.

Sincerely,

Christian Dawson
Executive Director
Internet Infrastructure Coalition