RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 2, 2026

General Joshua M. Rudd, USA
Director, National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755

Dear General Rudd:

I am writing to request the National Security Agency (NSA) update existing public guidance to address an important cybersecurity gap that leaves U.S. government officials, businesses, journalists, and activists vulnerable to surveillance by foreign adversaries. While commercial Virtual Private Networks (VPNs) are recommended by federal agencies and widely marketed as shields against online spying, standard consumer VPNs do not sufficiently protect users from sophisticated adversaries. Other, more secure alternatives are widely available.

In the attached July 21, 2026, letter, the Office of the Director of National Intelligence (ODNI) acknowledged that VPNs are a helpful component of basic cyber hygiene. ODNI properly cautioned that information about a VPN user remains exposed to the VPN company itself, which may record and store their private browsing histories. While ODNI's advice correctly stressed the importance of evaluating VPN providers' logging policies and encryption, it overlooked the importance of the VPN service's architecture against sophisticated foreign threats.

A September 2025 Cybersecurity Advisory, authored by the NSA and other U.S. and allied agencies, warned that PRC state-sponsored cyber threat actors were targeting networks globally including telecommunications, government, and military networks, with a focus on large backbone routers of major telecommunications providers as well as provider edge and customer edge routers. The attached Congressional Research Service (CRS) memo highlights the specific risk to VPNs of such network-level access, cautioning that "encryption strength alone does not protect users from an advanced, persistent threat conducting bulk traffic collection," because "even perfectly encrypted traffic reveals metadata (e.g., source, destination, timing, and volume) that can be correlated across a network to deanonymize users without ever breaking the [encryption]."

Defending against this surveillance threat is a challenge the United States Government recognized decades ago. In the 1990s, researchers at the U.S. Naval Research Laboratory created "Onion Routing"—which later became the open-source Tor network—specifically to protect U.S. military communications from traffic analysis by foreign adversaries. By routing user traffic through multiple servers and using other countermeasures, modern privacy enhancing technologies such as Tor can better prevent powerful foreign adversaries from correlating entry and exit data to unmask users.

According to CRS, "a single-hop VPN, however strongly encrypted, offers essentially no protection against an adversary who can compel… or infiltrate that one provider," whereas "multi-hop and mixnet architectures directly target and mitigate this weakness" by preventing any single server from knowing both the originating identity and the final destination.

Americans facing advanced foreign threats—including government personnel, defense contractors, journalists, and human rights defenders—deserve clear, honest advice about how best to protect their communications from surveillance by foreign adversaries. To that end, I request that you update NSA's existing public guidance on VPN configurations to address this issue. I also request that you provide me with unclassified, written responses to the following questions by October 14, 2026:

1. Are standard, single-hop commercial VPNs sufficient to protect Americans' sensitive digital footprints against foreign adversaries capable of monitoring internet backbones?
2. Does the NSA assess that Americans facing heightened surveillance threats, such as government officials, are better protected from foreign state-level traffic analysis when using multi-hop anti-surveillance tools—such as Apple Private Relay, Tor or Nym—rather than standard commercial VPNs?
3. What technical security features—including random delays, padding, and cover traffic—are essential to protect against surveillance by foreign adversaries, and how does the NSA rate the effectiveness of multi-hop proxy systems, like Apple Private Relay, relative to onion-routing and mixnet architectures, such as Tor and Nym?

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian and Shreyas Gandlur in my office.

Sincerely,

Ron Wyden
United States Senator