December 14, 2021

The Honorable Nancy Pelosi
Speaker of the House
U.S. House of Representatives

The Honorable Chuck Schumer
Majority Leader
U.S. Senate

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives

The Honorable Mitch McConnell
Minority Leader
U.S. Senate

The Honorable Adam Smith
Chairman
U.S. House Armed Services Committee

The Honorable Jack Reed
Chairman
U.S. Senate Armed Services Committee

The Honorable Mike Rogers
Ranking Member
U.S. House Armed Services Committee

The Honorable James Inhofe
Ranking Member
U.S. Senate Armed Services Committee

Dear Congressional Leaders:

The undersigned civil society groups write to express our strong support for the Malinowski-Meijer Amendment that had been included earlier this fall in the House-passed National Defense Authorization Act for Fiscal Year 2022 (Section 6467 in H.R. 4350). While we are disappointed that the provision was not included in the final NDAA measure that will likely soon clear Congress, we urge you to support including this bipartisan legislation in other must-pass legislation being considered by Congress. The legislation sponsored by Rep. Tom Malinowski and Rep. Peter Meijer would ban the use of federal funds to weaken encryption or intentionally insert backdoors and other vulnerabilities into our software and hardware devices.

As organizations committed to defending Internet freedoms, privacy, and other civil liberties, we share the fundamental understanding that online communications and commerce require our personal and financial information to be safe from intruders and eavesdroppers. End-to-end encrypting messages and data—which scrambles the information so that only the true sender and intended recipient are able to decode and access it—promotes the confidentiality, authenticity, privacy, and security of our communications and commerce transactions.

Around the world, ordinary people as well as members of persecuted communities, dissidents, whistleblowers, human rights defenders, and journalists rely on strong encryption to freely express themselves, exchange ideas and goods, organize, and criticize governmental actions without fear of retribution. Recognizing the importance of encryption to human rights, the U.S. government has spent millions equipping activists around the world with technologies to allow

them to communicate securely. Strong encryption is also essential to cybersecurity, protecting our communications devices from being hijacked, contaminated with ransomware, disabled, or otherwise abused.

Nonetheless, U.S. law enforcement and intelligence agencies are continuing their efforts to pressure and even coerce technology and telecommunications companies into creating supposedly secret backdoor access into people's communications and data for the government's easy access, or client-side scanning workarounds to obtain or access the information before encryption. These government demands persist despite the existence of other tools and methods that law enforcement has at its disposal. But as experts have repeatedly warned, there is no such thing as a secret or safe encryption backdoor or workaround; such self-inflicted security weaknesses inevitably get discovered and hijacked by bad actors of all stripes.

That is why the Malinowski-Meijer Amendment is vital and deserving of your endorsement. It is common sense legislation that would prohibit the federal government from spending taxpayer dollars to deliberately make everyone's personal communications and data more vulnerable to intrusions, theft, abuse, or exploitation.

Numerous cautionary tales illustrate the need for the Malinowski-Meijer Amendment to bolster cybersecurity and warn against governmental attempts to jeopardize it for everyone just to give the federal government yet another way to easily surveil and monitor a few. For instance, backdoors built into telecommunications switches in Greece for "lawful access" by the government were later hijacked to spy on Greek public officials. The Juniper security breach that came to light earlier this year—after a backdoor allegedly promoted by the National Security Agency into a major network security company's products was later hijacked by foreign hackers—is just the latest example of the risks of backdoors.

It is time for Congress to make our online communications and data more secure and private, not move in the opposite direction by funding government schemes to deliberately require providers to compromise everyone's cybersecurity.

For all these reasons, we urge you to enact the Malinowski-Meijer Amendment to protect strong encryption at the earliest opportunity. If you have any questions or comments, we stand ready to assist you.

Sincerely,

Access Now
American Civil Liberties Union
Electronic Frontier Foundation
Internet Society
New America's Open Technology Institute
Project On Government Oversight
Reform Government Surveillance