November 5, 2025

The Honorable Roger F. Wicker
Chairman
Senate Armed Services Committee

The Honorable Jack Reed
Ranking Member
Senate Armed Services Committee

The Honorable Mike Rogers
Chairman
House Armed Services Committee

The Honorable Adam Smith
Ranking Member
House Armed Services

Re: Streamlining procurement for secure collaboration and communication technology

Dear Chairmen Wicker and Rogers and Ranking Members Reed and Smith:

As the House and Senate negotiate the National Defense Authorization Act for Fiscal Year 2026, we urge you to support and retain Section 6612 of S.2296. This provision promotes the procurement of secure communications technology to protect our servicemembers and sensitive information from advanced cyber threats, at home and abroad. It also sets mandatory cybersecurity standards for the Pentagon's collaboration and communication software, saves taxpayers money by increasing software opportunities for the Pentagon, and ensures maximum innovation by breaking the anti-competitive lock-in effect caused by proprietary, walled-garden ecosystems.

The need for mandating the most secure collaboration systems for our military is clear given the increasing volume of successful hacks of U.S. government data resulting from foreign adversaries compromising the systems of government contractors. As the Cyber Safety Review Board documented, hackers working for the Chinese government compromised the Microsoft-hosted email accounts of several federal agencies in May 2023, including the Departments of State and Commerce. The hackers were able to access the communications of Cabinet officials and download approximately 60,000 emails from the State Department alone. In another, more recent incident, Chinese government hackers known as “Salt Typhoon” compromised the systems of major telephone companies in 2024, including AT&T and Verizon, successfully tapping the phones of Donald J. Trump and JD Vance, nominees for President and Vice-President respectively, and Members of Congress. While the hackers were able to tap calls and steal phone records, Mr. Vance stated in an October 31, 2024 interview with Joe Rogan that most of his communications remained secure in spite of the hack of his phone company, because he used the end-to-end encrypted messaging app Signal to communicate.

The lesson from these hacks is that without end-to-end encryption protecting government communications, a single hack of a service provider can enable foreign governments to surveil

senior U.S. government officials. Implementing stronger standards, including requirements for end-to-end encryption in collaboration systems, would protect U.S. government communications by ensuring that no one other than the sender and each intended recipient can access the decrypted communication, regardless of the transport technology used and the intermediaries or intermediate steps along the sending path. This standard would help ensure that even if servers are compromised, communications sent over those networks would remain protected from foreign surveillance. Among other cybersecurity requirements, this provision would require the Pentagon to use end-to-end encrypted communications technology when it is available, protecting warfighters' communications even if service providers are hacked.

Expanding the Pentagon's options for private communications providers will increase competition, lower costs, and prevent massive tech companies from locking it into wasteful spending through incompatible systems. For years, major tech companies have offered the same services like Microsoft Teams, Google Docs, Webex, Zoom, and a few others. Each of these platforms operates within its own set of siloed systems, creating inefficiencies by vendor-locking the millions of people at the Department of Defense into artificially scarce ecosystems, or forcing them to share sensitive information across multiple channels. To fix this pervasive issue and increase efficient collaboration, this provision mandates that standards for collaboration technology purchased by the Pentagon include a requirement for interoperability. This requirement will permit offices within the Pentagon to procure newer, better, or less-expensive systems in the future, and still be able to securely communicate with others in the Department using other systems. In addition to saving taxpayer money, mandating interoperability in procurement standards will force companies to make the best products available to the government, keeping our servicemembers and our nation secure.

The speed at which new offensive technologies are created is only accelerating, and Congress should incentivise industry practices that meet the moment. By implementing these standards, Congress will send a message to American companies that the Pentagon will only buy the best systems on the market, and open the door to new companies that create better products. America is at its best when it gives smaller, innovative companies the chance to offer cutting-edge solutions and compete with the legacy corporations, and our military will benefit by opening the door to such innovation.

We strongly urge you to protect America's national security and our sensitive information by supporting and retaining Section 6612 of S.2296, the National Defense Authorization Act for Fiscal Year 2026.

Sincerely,

American Economic Liberties Project

Asian Americans Advancing Justice | AAJC
Center for Democracy & Technology
Consumer Choice Center
Cory Doctorow
Demand Progress
dmarcian
Due Process Institute
Gate 15
Matrix.org Foundation
Open Markets Institute
Paperclip Inc.
Project for Privacy and Surveillance Accountability
Proton
Public Citizen
Public Knowledge

cc: Senate Majority Leader John Thune, Speaker of the House Mike Johnson, Senate Minority Leader Chuck Schumer, House Minority Leader Hakeem Jeffries