ROBERT MENENDEZ, NEW JERSEY, CHAIRMAN

BENJAMIN L. CARDIN, MARYLAND
JEANNE SHAHEEN, NEW HAMPSHIRE
CHRISTOPHER A. COONS, DELAWARE
CHRISTOPHER MURPHY, CONNECTICUT
TIM KAINE, VIRGINIA
EDWARD J. MARKEY, MASSACHUSETTS
JEFF MERKLEY, OREGON
CORY A. BOOKER, NEW JERSEY
BRIAN SCHATZ, HAWAII
CHRIS VAN HOLLEN, MARYLAND

JAMES E. RISCH, IDAHO
MARCO RUBIO, FLORIDA
RON JOHNSON, WISCONSIN
MITT ROMNEY, UTAH
ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY
TODD YOUNG, INDIANA
JOHN BARRASSO, WYOMING
TED CRUZ, TEXAS
MIKE ROUNDS, SOUTH DAKOTA
BILL HAGERTY, TENNESSEE

United States Senate
COMMITTEE ON FOREIGN RELATIONS
WASHINGTON, DC 20510–6225

July 13, 2021

The Honorable Antony J. Blinken
Secretary of State
U.S. Department of State
2201 C Street, N.W.
Washington, DC 20520

Dear Secretary Blinken,

I am deeply concerned about the national security implications of the recent wave of ransomware attacks, particularly that which exploited the Kaseya technology firm over the July 4th weekend. While I commend President Biden's statement to President Putin that Russia must take action to disrupt cybercriminals operating in Russia, and I applaud your efforts to discuss with Russian officials norms and rules that govern responsible conduct in cyberspace, the United States must remain clear-eyed about the Russian Federation's tactics and motivations in cyberspace. The administration has many authorities with which to act, including congressionally mandated sanctions under the Countering America's Adversaries Through Sanctions law (P.L. 115-44). I urge you to fully implement these sanctions authorities and mandates in response to these attacks as they happen, because without significant pressure from the United States and its allies, the Kremlin is unlikely to curb the cybercriminals it currently shelters.

From hospitals in California to schools and police departments in New Jersey, American businesses, infrastructure operators, and government agencies face significant digital risk and pressure. Operating in many cases from Russian soil, and through infrastructure that the Russian government monitors and controls, ransomware gangs have crippled or put at risk some of our most critical infrastructure, including water utilities, meatpacking plants, and one of the nation's largest fuel pipelines. According to the National Institute of Standards and Technology, cybercrime costs the United States hundreds of billions of dollars each year in economic losses. The related harm to public health and safety is incalculable, and can only be expected to grow as digital technologies become more intertwined in our daily lives. U.S. allies and partners are also suffering: just over a week ago, the Kaseya ransomware attack forced hundreds of Swedish supermarkets to close.

Russia is a hotbed for this dangerous activity. Ransomware gangs, such as DarkSide and REvil, operate freely in Russia. While I am not currently aware of evidence linking these groups directly to activities of or from the Russian state, experts believe that Russian cybercriminals act with the Kremlin's tacit approval and program their malware to avoid attacking computers in Russia and other nearby countries, knowing that the Russian authorities will tolerate them as long as they cause their damage elsewhere. As a matter of U.S. national security, this is unacceptable.

By allowing cybercriminals to operate with impunity, the Kremlin threatens international stability, undermines international institutions, and disregards international norms. As President Biden stated last month in Geneva, "responsible countries need to take action against criminals who conduct ransomware activities on their territory." The United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace, which counts Russia among its contributors, emphasized in this year's report that countries should "take all appropriate and reasonably available and feasible steps to detect, investigate and address" known cybercriminal activity emanating from their borders. But in practice, the Kremlin ignores this basic principle, and America and its allies pay the price.

I support robust diplomatic engagement with Russia on cybersecurity and other critical national security issues—but we must see results and exact clear and enforceable costs for continued violations. In the upcoming U.S.-Russia dialogue on these issues, I expect the administration will underscore the Kremlin's responsibility to curb the activities of cybercriminal gangs and other malign cyber actors operating from its territory, consistent with well-established international norms that Russia itself has endorsed. I also expect that you will make clear the specific and significant consequences if cyber and ransomware attacks continue, following on President Biden's statement that the United States will take necessary action to defend its people and its critical infrastructure.

I look forward to receiving a briefing from you following the upcoming U.S.-Russia dialogue so that we can consult on appropriate next steps and to working with you and the Department on this important issue.

Sincerely,

Robert Menendez
Chairman