COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Opening Statement of Vice Chair Ritchie Torres (D-NY)

Mobilizing Our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats

April 5, 2022

Today, the Committee is meeting to examine how we can better secure our Nation's critical infrastructure against Russian cyber threats. Just over one month ago, Russian troops launched an unprovoked, unjustified invasion of Ukraine. The United States and its allies responded swiftly and decisively, imposing harsh sanctions against Russian financial institutions, Russian government leaders and oligarchs, and even Vladimir Putin himself.

The Biden administration has also banned the import of Russian crude oil, petroleum, and natural gas; imposed export controls of critical technologies; and worked with our allies to ban Russia's largest banks from SWIFT. In time, these restrictions — together with additional actions taken by the United States and its allies — will cripple the Russian economy and undermine Putin's ability to continue his ill-conceived military operation in Ukraine. As Russia continues to struggle under the weight of sanctions imposed by the world's democracies, we must consider the potential risks to the homeland.

Over the past decade, Russia has demonstrated its ability and willingness to use cyber tools to advance its global agenda. It has used its neighbors in Eastern Europe as testbeds for deploying its cyber capabilities to interfere with elections, spread disinformation, and disrupt critical infrastructure. In 2015 and 2016, for example, Russian hackers temporarily knocked out power to over 200,000 Ukrainians. In 2017, Russia unleashed NotPetya to disrupt Ukraine's financial system, but the malware affected networks across critical infrastructure sectors globally, including in the United States.

Russia's willingness to deploy its cyber capabilities against the United States is well-documented. Since at least 2008, the intelligence community has warned of Russia's formidable cyber capabilities in its annual threat assessment. In 2017, the Intelligence Community concluded that the Russian government had attempted to interfere in the 2016 Presidential elections – engaging in both information operations and targeting election infrastructure. The following year, DHS and FBI warned entities in a range of sectors — from energy and aviation to water and critical manufacturing — that the Russian government was attempting to gain access to their networks. Despite these warnings, the Federal Government and its private sector partners have been slow to chart an enduring course for strategic partnership.

Historically, the Federal Government has struggled to demonstrate the security value of public-private partnerships. Meanwhile, the private sector has been reluctant to fully engage and feared new regulations. One of the most frustrating challenges we face is the lack of urgency to act based on intelligence alone. Too often, it has taken a major incident to force change.

The SolarWinds supply-chain attack is a good example. It forced a collective shift from admiring policy problems to solving them. The President issued an Executive Order overhauling and modernizing the Federal Government's approach to securing its networks.

Congress has also stepped up. It has increased cybersecurity funding and provided the Administration new authorities – including incident reporting and CyberSentry – that will help detect and eradicate malicious cyber campaigns faster. And the private sector has come to the table to work with the Federal Government in new ways.

The administration, Congress, and our private-sector partners have acted with urgency over the past year and left us better prepared to defend U.S. networks. But there is still room to improve.

First, the Biden administration has engaged in unprecedented cyber-threat information and intelligence sharing with critical infrastructure owners and operators in advance of and during Russia's unprovoked invasion of Ukraine. Moving forward, the government and private sector must assess the effectiveness of existing partnerships and continue to deepen strategic collaboration to defend against current and future cyber threats.

Second, the administration has undertaken historic initiatives to raise the cybersecurity posture across all 16 critical infrastructure sectors, which varies dramatically due to a range of factors from resources to regulation. To effectively defend against Russian cyber threats, the Federal Government must tailor its support to, and collaboration with, critical infrastructure sectors to their varying degrees of capability.

Toward that end, I was pleased to see the President's budget proposed a new competitive grant program aimed at raising the cybersecurity posture of certain critical infrastructure sectors. Finally, the Federal Government and the private sector must work together to harness the security gains realized as we defend against Russian cyber threats in order to establish a new, heightened security baseline.

# # #

Media contact: Adam Comis at (202) 225-9978