REMARKS OF
CHAIRWOMAN JESSICA ROSENWORCEL
TO THE CYBERSECURITY FORUM OF INDEPENDENT AND EXECUTIVE BRANCH REGULATORS
APRIL 8, 2022

Good morning. It's great to be with you, and it's great to kick off the first principals-level meeting of this Forum.

The first thing I want to say to all of you is: "Thank you." A few months ago, we put out a call to relaunch this Cybersecurity Forum, not knowing what kind of response we would get. Your agencies answered that call enthusiastically and without hesitation. For that, I am truly grateful.

Since then, many have asked why it is important that we revitalize this group now. To that, I would say the membership *is* the message. Cybersecurity is an issue for everyone, everywhere. We are revitalizing this group and we are doing it now because no threat facing our national and economic security has grown as fast as the threat of cyberattacks, and because we know that no single entity can meet this challenge alone.

But here's the good news. We have a lot of momentum behind us already. As a nation, during the past year, we have demonstrated that combatting cyberattacks is a top priority. We've elevated seasoned cybersecurity experts and restructured agencies. We've hardened government and private infrastructure in the wake of the Colonial Pipeline ransomware attack. We've removed critical roadblocks that private companies can face when sharing information with the government. We've demanded better security standards from software companies when they sell to federal users. Plus, internationally, we've rallied our allies to respond to ransomware attacks and to update multilateral cyber policies.

Congress has led on these efforts, too. The American Rescue Plan Act funds new cyber risk mitigation programs. The K-12 Cybersecurity Act studies the threat that cyberattacks pose on our schools. The Infrastructure Investment and Jobs Act includes new programs to train staff, incentivize greater private sector cooperation, and upgrade state, local, territorial, and Tribal governments' cybersecurity infrastructure across the U.S. The Cyber Incident Reporting for Critical Infrastructure Act creates the first holistic framework for reporting cyber incidents so that the federal government can help respond. And the 2022 National Defense Reauthorization Act commissions new reports to study the nation's cyber posture and initiates new efforts to eliminate legacy software systems, among other things.

All of this activity means we have better visibility, better tools, and better resources at our fingertips. Now we must organize and build on this momentum.

When this body was first created in 2014, it was focused primarily on information sharing and self-regulatory approaches. The cyber threats to our critical infrastructure have evolved since then, so this group's mission should evolve to keep pace.

Our chief objective now is to harmonize how private sector industries implement essential cybersecurity controls and how independent and executive branch regulatory agencies can ensure their work advances those efforts.

We've identified two places to start, which we'll talk about with you today.

First, we'll discuss how this group can work on achieving greater consistency in the reporting of cyber incidents. Right now, there's a lot of fragmentation across sectors and jurisdictions in what information gets reported, when and how it is reported, and how that information can be used. So we'll discuss using this Forum as a place to work toward greater convergence on these matters.

Second, we'll discuss the role that this Forum can play to advance the goals of Executive Order 14028, which identifies a number of actions to improve the government's ability to protect against cyber threats.

We've got a great line-up to help kick off this work. We'll start with a briefing from National Cyber Director Chris Inglis. After that, we'll move to a discussion about harmonizing cybersecurity regulatory approaches led by Department of Homeland Security Under Secretary Rob Silvers and Acting Comptroller of the Currency, Michael Hsu. Then, we'll receive an update from Cybersecurity and Infrastructure Security Agency Executive Director Brandon Wales on the Russia-Ukraine crisis. Finally, we'll close with remarks from Deputy National Security Advisor Anne Neuberger.

Before we get started, I want to share one last thought. When it comes to cybersecurity, there is no question that the risks are real, the stakes are high, and our defenses need to evolve and improve. This Forum is part of the nuts-and-bolts work to help get us to where we need to be. It will be hard, and it won't be glamorous. But as President Truman famously said, "It's amazing what you can accomplish when you don't care who gets the credit." Let's honor those words and make progress—together.

It is my pleasure now to introduce the National Cyber Director, Chris Inglis.