WASHINGTON—Today, Deputy Secretary of the Treasury Wally Adeyemo delivered remarks at the semi-annual Joint session of the FBIIC (Financial and Banking Information Infrastructure Committee) and FSSCC (Financial Services Sector Coordinating Council) where he discussed Treasury’s unprecedented, year-long efforts that have bolstered public-private relationships to protect the Department and financial sector from cyber threats.

The Deputy Secretary’s remarks outlined significant steps the Department has taken the beginning of the Administration. These include modernizing Treasury’s IT systems with an elevated cybersecurity threat focus, as well as ramping up partnerships with the financial and regulatory sectors far ahead of Russia’s unprovoked invasion of Ukraine to ensure swift, coordinated responses to thwart cyber attacks. Deputy Secretary Adeyemo underscored the need to continue to fortify these partnerships and to remain vigilant in this time of heightened threats.

As prepared for delivery:

Thank you all for being here, and a special thank you to Ron Greene and the entire Mastercard team for hosting and for your leadership as chair of the FSSCC.

I spend a great deal of my time day-to-day thinking about some of our most persistent challenges, from how we safeguard national security against a range of threats to how we can use domestic economic policy to help addresses challenges from racial inequity to climate change. What these diverse policy areas have in common is that they require solutions beyond the capabilities of the public or the private sector alone—joint efforts are needed to get us to where we need to be.

When it comes to protecting our critical infrastructure, we know that the public and private sectors’ fates are often intertwined. We saw just last month that the same adversary that launched multiple waves of DDoS attacks at Treasury turned its attention to some of you a few
days later. This incident was a stark reminder that when it comes to cyber threats, we are in this together.

During the last 20 years of this partnership, FBIIC and FSSCC have set the standard for public-private collaboration, and we have made remarkable progress together.

One clear example of the importance and effectiveness of our work together is in our response to Russia’s invasion of Ukraine. Before and over the course of this unconscionable invasion, we have remained in close contact with many of you to provide critical updates, flag potential risks, and ensure we are giving you what you need to keep your systems secure.

In response to your feedback, Treasury partnered with national intelligence and law enforcement agencies to organize monthly classified briefings with FBIIC and FSSCC to provide updates on Russia’s cyber strategy and capabilities. Your firms also worked with us to scope the topics and tactical information in our intelligence series on lessons learned from this Russia experience.

With input and insight from you all, we have also been able to identify and respond to gaps in our existing infrastructure and processes.

Russia’s invasion of Ukraine and the international fallout it has caused have also demonstrated how interconnected the global financial sector is—and in turn, the global nature of the risks we face. To that end, we have made enhancing operational resilience in major global banking hubs and vulnerable regions a top priority.

But despite these efforts, I—like many of your CEOs—know we need to do more, and faster to ensure we keep pace in the growing threat environment we face.

Later this week, I will chair the end of year session of the “FBIIC Senior Leaders,” where we will set our goals for 2023. This year, we made great progress on critical issues like cloud adoption and federal response timelines. As we head into the new year, I am calling on FBIIC senior leaders to continue to drive our successful cloud and data protection workstreams forward, while building new initiatives that focus on other urgent, systemic risk issues. As part of this effort, it is imperative that FBIIC bring our FSSCC partners into these processes and deepen this partnership.

And to our FSSCC partners: I want to reiterate how valuable your coordination is and how much we rely on your insights and experiences. As we work to better integrate you into FBIIC workstreams, we are calling on you to continue to expeditiously share your information with...
Treasury and other federal government partners. Reporting cybersecurity issues and vulnerabilities early and often enables us to better protect the broader financial sector.

The challenges before us are sophisticated and often interrelated. We need to deepen and grow the partnership between public and private sectors to better respond to the challenges that we face together, building on the track record of success we’ve had together over the last year.

Thank you.