Testimony of Deputy Secretary of the Treasury Wally Adeyemo Before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate

April 9, 2024

As Prepared for Delivery

Chairman Brown, Ranking Member Scott, and members of the Committee, thank you for the invitation to join you here today. I want to thank you and the members of the committee for your willingness to work with us to address various threats to our national security.

I am here today because we need additional tools to protect the American people.

As we take steps to cut terrorist groups and other malign actors off from the traditional financial system, we are concerned about the ways these actors are using cryptocurrencies to try and circumvent our sanctions.

For example, five years ago, al-Qaeda and affiliated terrorist groups, largely based out of Syria, operated a bitcoin money laundering network using social media platforms to solicit cryptocurrency donations. After receiving virtual currency, they laundered the proceeds through various online gift card exchanges to be able to purchase what they needed to advance their violent agenda.

More recently, over the past year, we have seen the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) transfer cryptocurrency to Hamas and the Palestinian Islamic Jihad (PIJ) in Gaza. In addition, we have seen Hamas use virtual currencies to solicit small-dollar donations, and we have been able to take action against these networks.

Our problem is that actors are increasingly finding ways to hide their identities and move resources using virtual currency. What has always been true is that terrorists and other malign actors seek new ways to move their resources in light of the actions we are taking to cut them off from accessing the traditional financial system.

Today, because of the authorities Congress has provided us, we have a long track record of taking action to make it harder for these groups to use the traditional financial system to move money. We continue to use our authorities aggressively to cut off the illicit finance

networks that enable illicit actors worldwide, including Hamas and other Iran-backed proxies, Russian oligarchs, and ISIS, to name a few.

The more effective our targeting has been, the more reason there is for these terrorist groups to look into virtual assets. And, to be clear, it's not only terrorist groups, but state actors like the DPRK and Russia as well.

The DPRK, which through numerous complex state-sponsored cyber heists, is able to acquire, launder, and store illicit revenue. It relies on anonymity-enhancing technologies like mixers to hide the sources of its funds. And it leverages over-the-counter digital assets traders to acquire fiat currency. In addition, we've seen Russia increasingly turning to alternative payment mechanisms—including the stablecoin tether—to try to circumvent our sanctions and continue to finance its war machine.

While we have had some success in rooting out illicit finance in the digital asset ecosystem, we need to build an oversight and enforcement regime that is capable of preventing this activity as more terrorists, transnational criminals, and rogue states turn to digital assets. That's why we sent the Committee proposals to strengthen counter-terrorist financing authorities, and we look forward to working with the Committee on your ideas and proposals.

The options I sent over to the Committee in November focused broadly on three reforms.

- The first is the introduction of a secondary sanctions tool targeted at foreign digital asset providers that facilitate illicit finance.
- The second reform is centered on modernizing and closing gaps in existing authorities by expanding their reach to explicitly cover the key players and core activities of the digital assets ecosystem.
- Finally, a third reform addresses jurisdictional risk from offshore cryptocurrency platforms, which is a key challenge.

There is clear overlap between these proposals and the bipartisan bills coming out of this Committee. We agree that the use of these emerging technologies by illicit actors can have impacts on the national security, foreign policy, and economy of the United States. That's why the United States has a strong interest in ensuring that we have the necessary tools and authorities available and are ready to mitigate the risks in this quickly evolving ecosystem, including for dollar-based digital assets in particular.

While we continue to assess that terrorists prefer to use traditional financial products and services, we fear that without Congressional action to provide us with the necessary tools,

the use of virtual assets by these actors will only grow.

And while these actors today only use virtual assets for a fraction of their illicit activity, we know in other areas, illicit actors almost completely rely on virtual currencies. Over the past few years, ransomware attacks have only increased in scale, sophistication, and frequency. Treasury's Financial Crimes Enforcement Network found, based on BSA reporting, that more than $1 billion of ransomware payments were made exclusively using cryptocurrency in 2023. This not only has an impact on our national security but also on our economy.

We are grateful for the partnership of Congress and this Committee in helping Treasury root out illicit finance from the U.S. financial system and to hold illicit actors accountable. I look forward to today's discussion on how we can continue this work.

###