Periodic Report on the National Emergency
With Respect to Significant Malicious Cyber-Enabled Activities

I hereby report to the Congress on developments and expenditures relating to the national emergency declared in Executive Order 13694 of April 1, 2015, as amended by Executive Order 13757 of December 28, 2016, which blocks the property of certain persons engaging in significant malicious cyber-enabled activities. In accordance with section 204(c) of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1703(c), this report covers actions taken in the exercise of national emergency authorities under IEEPA, and implementing regulations set forth at 31 C.F.R. part 578 (the Cyber-Related Sanctions Regulations). It also covers expenses that are directly attributable to the exercise of those authorities, in accordance with section 401(c) of the National Emergencies Act (NEA), 50 U.S.C. 1641(c).

IEEPA Reporting (from February 7, 2020, through September 9, 2020)

1. On March 2, 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated, pursuant to the authorities referenced above, two Chinese nationals involved in laundering stolen cryptocurrency from a 2018 cyber intrusion against a cryptocurrency exchange. This cyber intrusion is linked to Lazarus Group, a North Korean state-sponsored malicious cyber group designated by OFAC in 2019. Specifically, OFAC designated Tian Yinyin and Li Jiadong for having materially assisted, sponsored, or provided financial, material, or technological support for a malicious cyber-enabled activity. Tian and Li were also designated for having materially assisted, sponsored, or provided financial, material, or technological support for Lazarus Group.

On June 16, 2020, OFAC designated six Nigerian nationals pursuant to the authorities referenced above.

On July 15, 2020, OFAC designated three individuals and five entities directly involved in furthering previously designated individual Yevgeniy Prigozhin's operations in Sudan and assisting his ability to evade sanctions. Prigozhin is the financier of the Internet Research Agency (IRA), the Russian troll farm that was designated by OFAC in 2018. Prigozhin is also believed to be the financier behind Private Military Company (PMC) Wagner, a designated Russian Ministry of Defense proxy force.

2. OFAC closed three licensing cases (which may take the form of specific licenses, license amendments, "return-without-action" letters, general information letters, interpretive guidance letters, denial letters, closed without determination letters, or withdrawals), and received reports of the blocking of 22 transactions totaling $199,000, pursuant to the authorities referenced above.

3. OFAC has continued to discuss this program during its numerous outreach events to the financial, securities, and international trade communities. Details of this program are available on the Department of the Treasury's website.

NEA Reporting (from April 2, 2020, through October 1, 2020)

4. The expenses incurred by the federal government that are directly attributable to the exercise of powers and authorities conferred by the declaration of the national emergency with respect to significant malicious cyber-enabled activities are reported to be approximately $1.04 million, most of which represent wage and salary costs for federal personnel. Personnel costs were largely centered in the Department of the Treasury, the Department of State, and the Department of Justice.

I shall continue to report periodically to the Congress on significant developments as required by law.

Steven T. Mnuchin

Steven T. Mnuchin

Department of the Treasury

Dated: SEP 2 9 2020