United States Senate
WASHINGTON, DC 20510

December 15, 2020

Secretary Steven T. Mnuchin
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

Dear Secretary Mnuchin:

We write to express our deep concern and to gather information about the serious cyber-attack, reportedly by actors related to or on behalf of Russian intelligence services, on systems at the Treasury and Commerce Departments that were widely reported on over the weekend. These media reports suggest that these attacks were comprehensive and historic and bad actors may have had access to critical U.S. government networks for many months. Since the weekend, media reports have made clear that the scope of the attack has widened to include the State Department, the Department of Homeland Security, the National Institutes of Health, and parts of the Pentagon.

In furtherance of our respective Committees' oversight work, we would like answers to a series of key questions about what appears to be a serious compromise of U.S. government systems, and what steps are being taken immediately by Treasury to mitigate the risks associated with this security breach. Most immediately, we would like answers to the following specific questions:

- Has the Treasury Department begun assessing all its computer systems for compromise? So far, which offices, bureaus, and departments were affected? Please detail the types of networks and services that were compromised, including their business purpose, whether internal or external facing, and the classification of each network compromised, along with an update on the status of such assessments.

- As a result of the compromised systems, what resources (e-mail, file systems, etc.) were accessible to the attackers? Please include, as far as you have been able to determine, the privileges the attackers had on each resource (read-only, modify, etc.). Specifically, is there evidence of compromise of the classified systems at the Treasury's Office of Intelligence and Analysis? If so, have you been able to determine what classified information was accessed and the associated risk to national security?

- When and how did the Treasury Department first learn of this security breach? Was any notification made to Congressional Leadership or Committees of Oversight? Have you sought assistance from the technical experts at the Cybersecurity and Infrastructure Security Agency (CISA)? If so, when did you ask CISA to intervene? Have you sought assistance from the technical experts from the Federal Bureau of Investigation's (FBI) Cyber Division? If so, when did you ask the FBI to intervene? Which agency and team is currently leading the incident response process?

- Is the Treasury Department security breach related to the compromise of SolarWinds software noted in CISA's Emergency Directive 21-01? FireEye, a respected cybersecurity firm, reports that SolarWinds software may have been compromised as early as Spring 2020. On what date do the Treasury Department's systems first appear to have been compromised?

- Does the Treasury Department employ in-house personnel properly trained in taking a forensic image of system memory and do they have tooling readily available to immediately do so? If so, have they completed the forensic analysis detailed in Action 1 of Emergency Directive 21-01? If not, who has the Treasury Department relied on to complete a similar forensic analysis?

- Has the Treasury Department completed the actions to limit damage from compromised SolarWinds software as detailed in Action 2 of Emergency Directive 21-01? If not, please detail the reasons and expected completion time. What other steps have you taken to mitigate risks posed by the SolarWinds software compromise?

- Once the U.S. government formally attributes the attack to specific actors, will the Treasury Department initiate a process to consider using the full panoply of economic, financial, cyber, and other sanctions tools Congress has provided to the Treasury Department, or other counter-measures, to respond appropriately?

- Has the Treasury Department begun assessing the overall effects on US national and economic security of this breach? Has the Department informed incoming Biden Treasury transition officials with appropriate clearance of the nature and extent of the breach, and prepared them by providing extensive information on recommended next steps Treasury proposes to take to protect its system and mitigate any further damage?

Thank you for your consideration. We look forward to hearing from you.

Sincerely,

Sherrod Brown
Ranking Member of the Committee on
Banking, Housing and Urban Affairs

Ron Wyden
Ranking Member of the Committee
on Finance