United States Senate
COMMITTEE ON FOREIGN RELATIONS
WASHINGTON, DC 20510–6225

December 22, 2020

The Honorable Michael Pompeo
Secretary of State
U.S. Department of State
2201 C Street, N.W.
Washington, DC 20520

Dear Secretary Pompeo,

I am writing to request a classified briefing for Members of the Senate Foreign Relations Committee by appropriate senior Department officials on the Russian-backed SolarWinds breach and the cyber infiltration of U.S. government and private sector systems and networks as soon as possible after the Senate reconvenes on January 4, 2021.

It is critical that the Senate Foreign Relations Committee receive a briefing on the extent of the security breach and the efforts that the Department is taking to mitigate its impacts and defend against future attacks. Furthermore, it is essential that critical sectors within private industry and the American public more broadly understand the nature of the threat that our nation faces from the Kremlin, and their persistent exploitation of cyberspace, the Internet, and social media for their malign ends.

While several other cabinet agencies that are victims of this cybersecurity breach have publicly acknowledged having been attacked, to date the Department of State has been silent on whether its computer, communication and information technology systems were compromised. For the Committee briefing I would therefore appreciate better understanding of:

1. The Department's assessment of the nature, scope, design, and intent of the breach, including those responsible for the operation;
2. When the Department of State became aware of the SolarWinds breach, if the Department has experienced similar intrusions in 2019 or 2020, and whether any such hacks breached departmental systems;
3. The Department's assessment of what systems or materials that may have been compromised, including as it relates to the confidentiality and integrity of data, mapped, exfiltrated, or otherwise placed at risk, and the steps that have been and will be taken to mitigate any such damage;
4. Any on-going risk that cyber-intruders may still persist in any departmental systems, including on-going efforts to identify and expel any intrusions, and to manage any potential damage or exposure;
5. Any cooperation and coordination with other relevant USG agencies or offices to address the attack, identify attackers or breaches, conduct diagnostics, and repair departmental

systems, including by granting other appropriate elements of the USG access to departmental systems for such purposes;

6. The steps the Department is taking to assess risks within the cybersecurity supply chain and any steps the Department considers necessary to mitigate those risks;
7. An assessment of the breach of and risks to cyberphysical devices;
8. Any steps currently being taken or contemplated to prevent future attacks; and,
9. Foreign policy measures and diplomatic recommendations or other steps recommended or taken by the Department to respond to the SolarWinds breach and to deter any future such attacks.

Mr. Secretary, I know you share my concerns about the potential for damage that this attack presents to our nation and to the Department of State. I look forward to working with you to arrange for a briefing and a fuller discussion of these issues.

With all the best for a safe, happy, and healthy new year.

Sincerely,

Robert Menendez
Ranking Member