DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

December 30, 2024

The Honorable Sherrod Brown
Chairman
Committee on Banking, Housing
and Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Tim Scott
Ranking Member
Committee on Banking, Housing
and Urban Affairs
United States Senate
Washington, DC 20510

Dear Chairman Brown and Ranking Member Scott:

In accordance with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA) and criteria provided in Office of Management and Budget (OMB) Memorandum 24-04, this letter provides notice that the Department of the Treasury (Treasury) has determined that a major incident occurred.

On December 8, 2024, Treasury was notified by a third-party software service provider, BeyondTrust, that a threat actor had gained access to a key used by the vendor to secure a cloud-based service used to remotely provide technical support for Treasury Departmental Offices (DO) end users. With access to the stolen key, the threat actor was able override the service's security, remotely access certain Treasury DO user workstations, and access certain unclassified documents maintained by those users.

Treasury has been working with the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Intelligence Community, and third-party forensic investigators to fully characterize the incident and determine its overall impact. CISA was engaged immediately upon Treasury's knowledge of the attack, and the remaining governing bodies were contacted as soon as the scope of the attack became evident. Based on available indicators, the incident has been attributed to a China state-sponsored Advanced Persistent Threat (APT) actor.

The compromised BeyondTrust service has been taken offline and at this time there is no evidence indicating the threat actor has continued access to Treasury information. The investments we have made using discretionary appropriations provided under the Cybersecurity Enhancement Account (CEA) have helped ensure we have strong incident processes and access to detailed logs to support our incident response efforts.

In accordance with Treasury policy, intrusions attributable to an APT are considered a major cybersecurity incident. More details will be made available in our 30-day supplemental report to this notification, which we are required to provide under FISMA and OMB guidance.

If you have any questions, please direct your staff to contact Treasury's Office of Legislative Affairs at 202-622-1900 or legaffairs@treasury.gov.

Sincerely,

Aditi Hardikar
Assistant Secretary for Management
U.S. Department of the Treasury