



U.S. Senate Majority Leader Charles E. Schumer
322 Hart Senate Office Building
Washington, D.C. 20510

April 5, 2021

Re: New York State Government Purchase of Restricted IT Equipment

Dear Senator Schumer,

Thank you for your leadership on U.S-China policy. I write out of concern for the privacy and security of New Yorkers and the hope that New York can become a new nexus of [semiconductor design and manufacturing](#). Extensive research conducted by my organization, [China Tech Threat](#), shows that while federal policymakers have long focused on curtailing security threats posed by Chinese-government owned information technology (IT) firms, those same safeguards have not been adopted by state and local governments, including New York.

An [analysis](#) of New York State procurement records found that the New York state government has spent more than \$28 million on technology products and services by Chinese state-owned tech manufacturers Lenovo and Lexmark. Both companies have ownership ties to the Chinese government and Chinese Communist Party. This concerning finding comes as the state plans to allocate [\\$23.5 billion in federal American Rescue Plan funding](#), much of which will be used to upgrade its IT systems, authorities should proactively audit its networks, remove vulnerable components and source new products exclusively from trust vendors in democratic nations. Additionally, the New York Office of General Services has requested bids for a significant hardware technology purchase, which will likely be decided in the weeks ahead.

China Tech Threat inquired to the New York's Office of General Services (OGS) as to whether the state's procurement policy considers federal restrictions on its technology providers; whether it weighs the impact of foreign adversarial state-owned enterprises; and how it evaluates data security in its procurement. The [letter](#) cites a 2019 Department of Defense Inspector General (DODIG) [report](#) noting that Lenovo products have been restricted, investigated, or deemed vulnerable by the DOD Information Network in 2018, the Joint Chiefs of Staff Intelligence Directorate in 2016, the Department of Homeland Security in 2015, and the State Department in 2006. Similarly, the DODIG notes that Lexmark has "connections to Chinese military, nuclear, and cyberespionage programs." This inquiry is still pending.

I am encouraged by your leadership to expand our country's leadership in competitiveness in next generation chip research and manufacturing and to boost funding to support these efforts. As the home to the world's financial markets and a diverse base of cutting-edge industries, New York is already a lucrative target for state-sponsored cyber-criminals—namely the Chinese military hackers—who are actively working to pilfer U.S.-made technology, government secrets and consumer data. As you seek to attract much of this job-creating investment to New York, I kindly request your support in determining what, if any, guardrails exist to prevent government purchases from Chinese state-owned manufacturers, whose products may contain built-in backdoors and other vulnerabilities.

Sincerely,

A handwritten signature in blue ink that reads "Roslyn Layton".

Roslyn Layton, Ph.D.
Co-Founder, China Tech Threat
roslyn@ChinaTechThreat.com